100 XP

Introduction

1 minute

Microsoft Cloud services are built on a foundation of trust, security, and compliance. The Microsoft Service Trust Portal provides a variety of content, tools, and other resources about Microsoft security, privacy, and compliance practices.

Microsoft also helps organizations meet their privacy requirements, with Microsoft Priva. Priva helps organizations safeguard personal data and build a privacy-resilient workplace.

In this module you'll learn about the Service Trust Portal and resources it provides, including audit reports, security assessments, and compliance guides that enable organizations to manage compliance. You'll learn about Microsoft's commitment to privacy and its privacy principles. Lastly, you'll learn about Microsoft Priva, which helps organizations meet their privacy goals.

After completing this module, you'll be able to:

- **Describe the offerings of the Service Trust Portal.**
- **Describe Microsoft's privacy principles.**
- **Describe Microsoft Priva.**

Next unit: Describe the offerings of the Service Trust portal

Continue

100 XP

Describe the offerings of the Service Trust portal

7 minutes

The Microsoft Service Trust Portal provides a variety of content, tools, and other resources about how Microsoft cloud services protect your data, and how you can manage cloud data security and compliance for your organization.

The Service Trust Portal (STP) is Microsoft's public site for publishing audit reports and other compliance-related information associated with Microsoft's cloud services. STP users can download audit reports produced by external auditors and gain insight from Microsoft-authored whitepapers that provide details on how Microsoft cloud services protect your data, and how you can manage cloud data security and compliance for your organization.

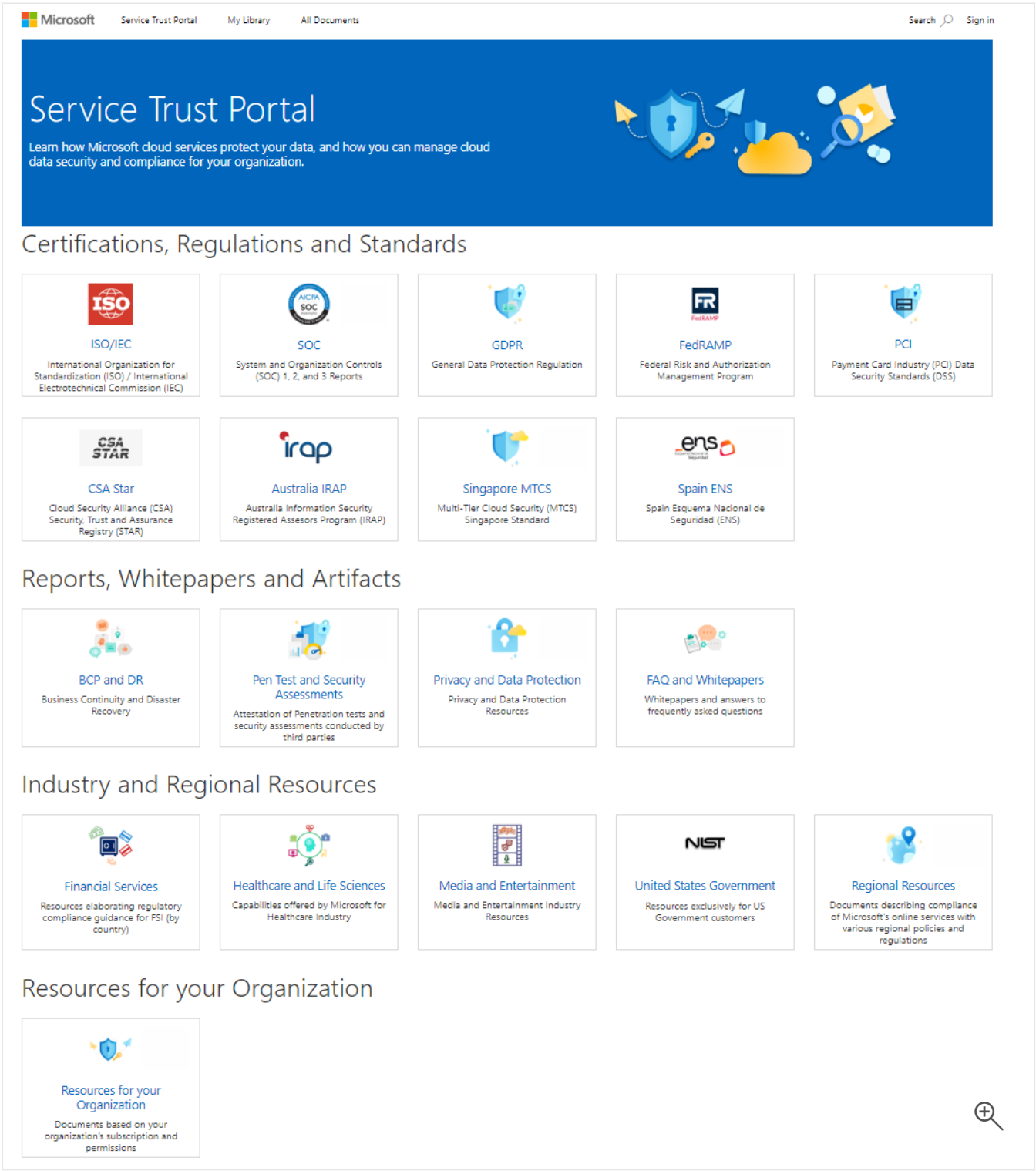
Accessing the Service Trust Portal

To access some of the resources on the Service Trust Portal, you must log in as an authenticated user with your Microsoft cloud services account (Azure Active Directory organization account) and review and accept the Microsoft non-disclosure agreement for Compliance Materials.

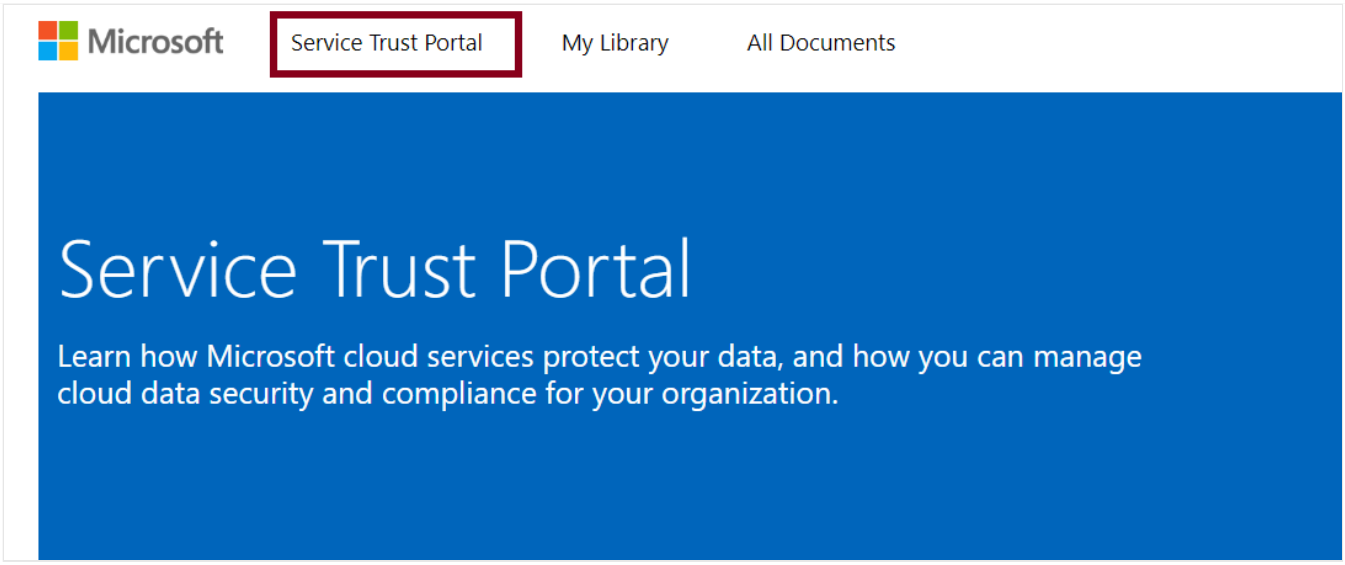
Service Trust Portal Content Categories

The Service Trust Portal landing page includes content that is organized into the following categories:

- **Certifications, Regulations, and Standards**
- **Reports, Whitepapers, and Artifacts**
- **Industry and Regional Resources**
- **Resources for your Organization**

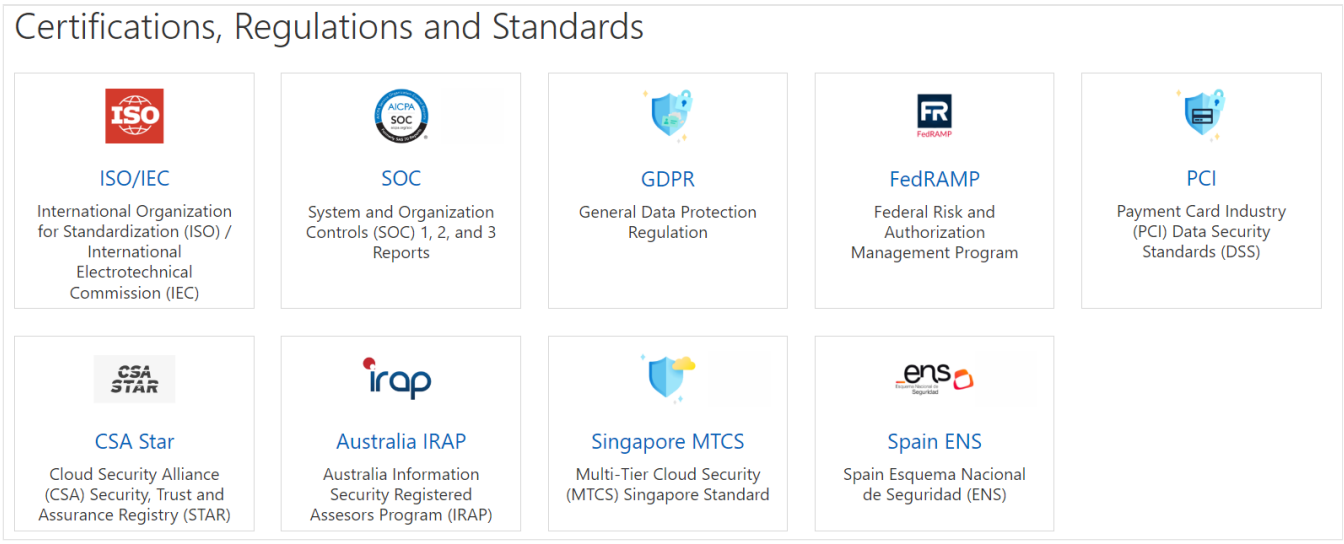


As users navigate to content in the different categories, selecting the Service Trust Portal link at the top of the page provides a quick way to get back to the home page.

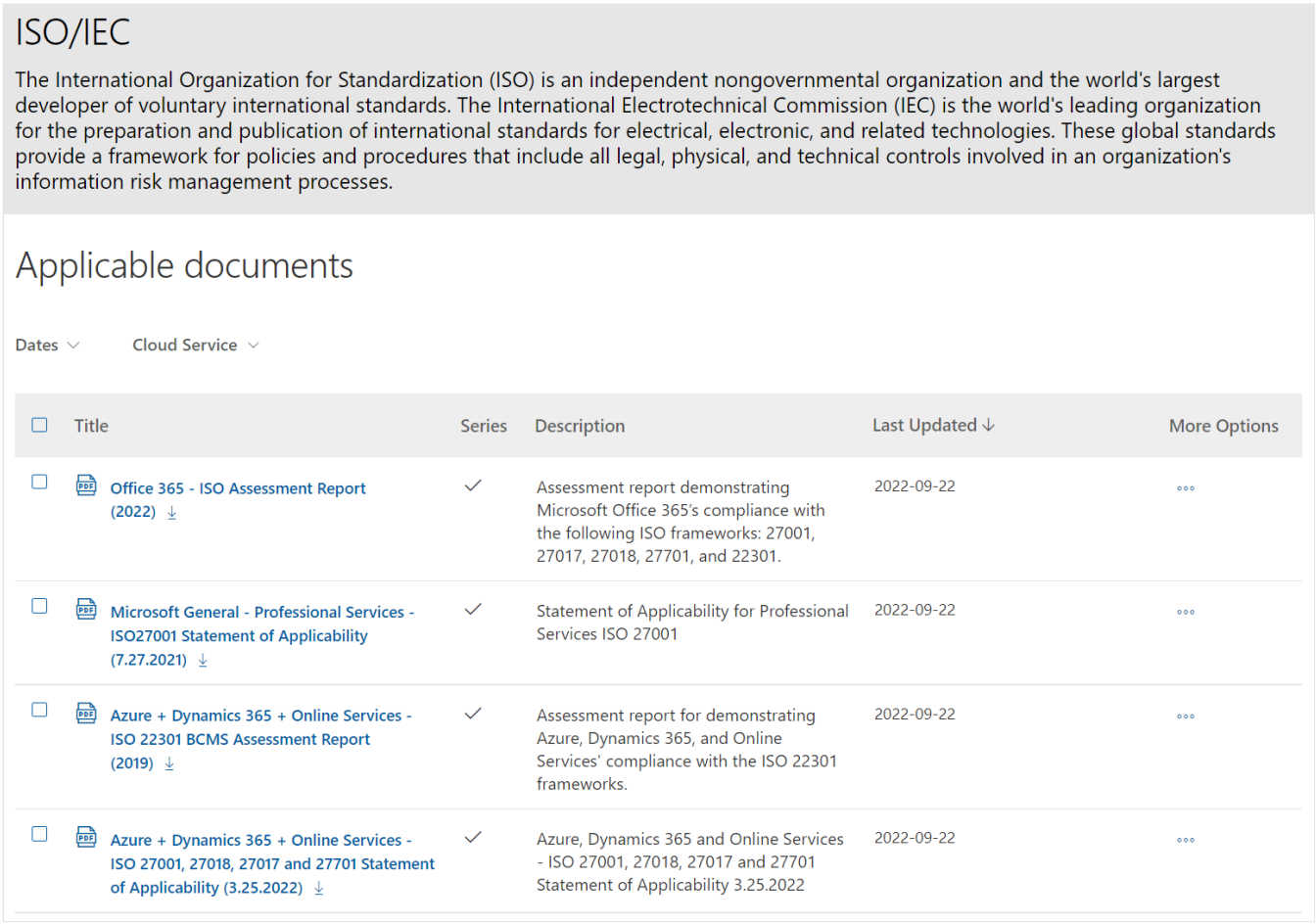


Certifications, Regulations and Standards

The certification, regulations, and standards section of the STP provides a wealth of security implementation and design information with the goal of making it easier for you to meet regulatory compliance objectives by understanding how Microsoft Cloud services keep your data secure.



Selecting a tile will provide a list of available documents, including a description and when it was last updated. The screenshot that follows shows some of the documents available by selecting the ISO/IEC tile.



Reports, Whitepapers, and Artifacts

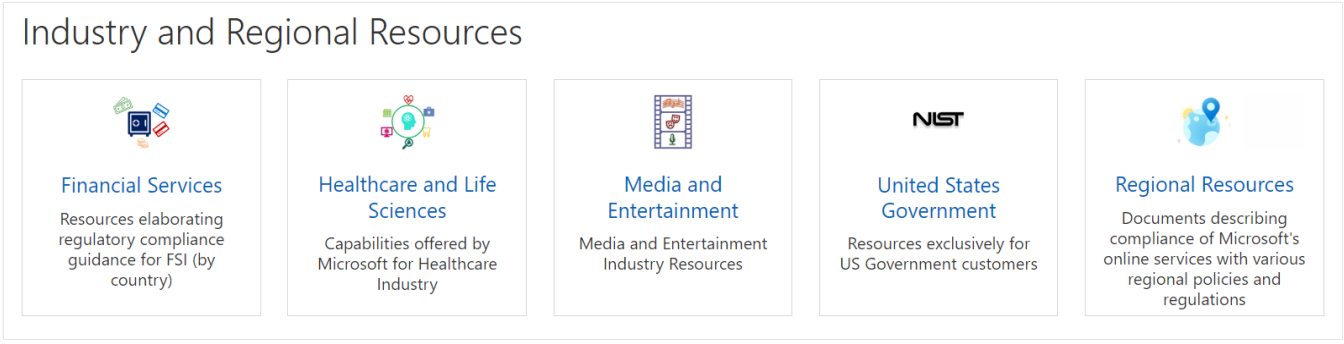
This section includes general documents relating to the following categories:

- **BCP and DR - Business Continuity and Disaster Recovery**
- **Pen Test and Security Assessments - Attestation of Penetration tests and security assessments conducted by third parties**
- **Privacy and Data Protection - Privacy and Data Protection Resources**
- **FAQ and Whitepapers - Whitepapers and answers to frequently asked questions**

Industry and Regional Resources

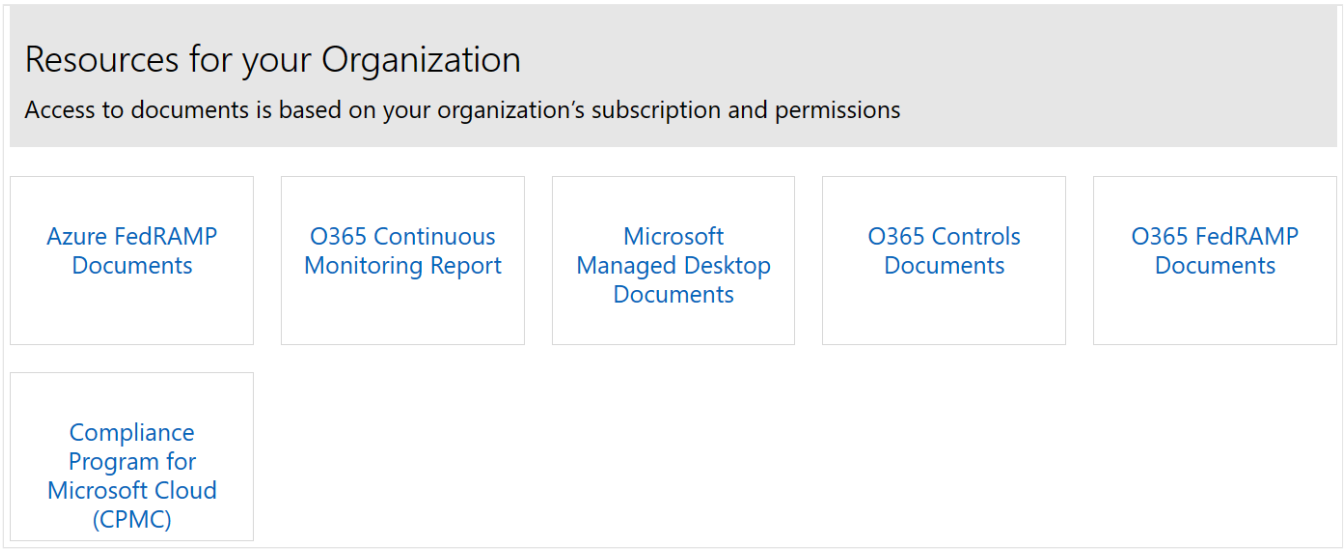
This section includes documents that apply to the following industries and regions:

- **Financial Services - Resources elaborating regulatory compliance guidance for FSI (by country/region)**
- **Healthcare and Life Sciences - Capabilities offered by Microsoft for Healthcare Industry**
- **Media and Entertainment - Media and Entertainment Industry Resources**
- **United States Government - Resources exclusively for US Government customers**
- **Regional Resources - Documents describing compliance of Microsoft's online services with various regional policies and regulations**



Resources for your Organization

This section lists documents applying to your organization (restricted by tenant) based on your organization's subscription and permissions.

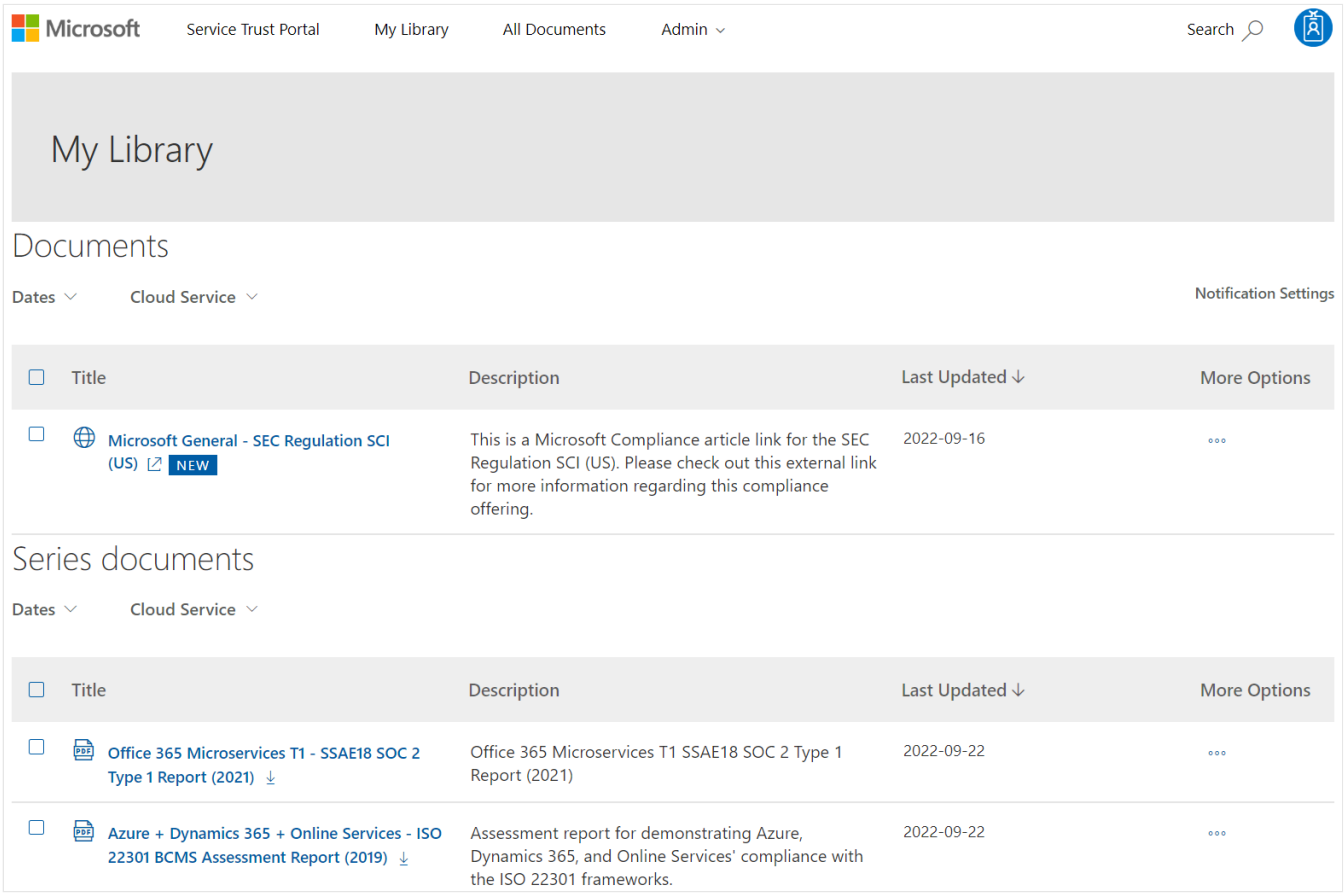


My Library

Use the My Library feature to add documents and resources on the Service Trust Portal to your My Library page. This lets you access documents that are relevant to you in a single place. To add a document to your My Library, select the ellipsis (...) menu to the right of a document and then select Save to library.

Additionally, the notifications feature lets you configure your My Library so that an email message is sent to you whenever Microsoft updates a document that you've added to your My Library. To set up notifications, go to your My Library and select Notification Settings. You can choose the frequency of notifications and specify an email address in your organization to send notifications to. Email notifications include links to the documents that have been updated and a brief description of the update.

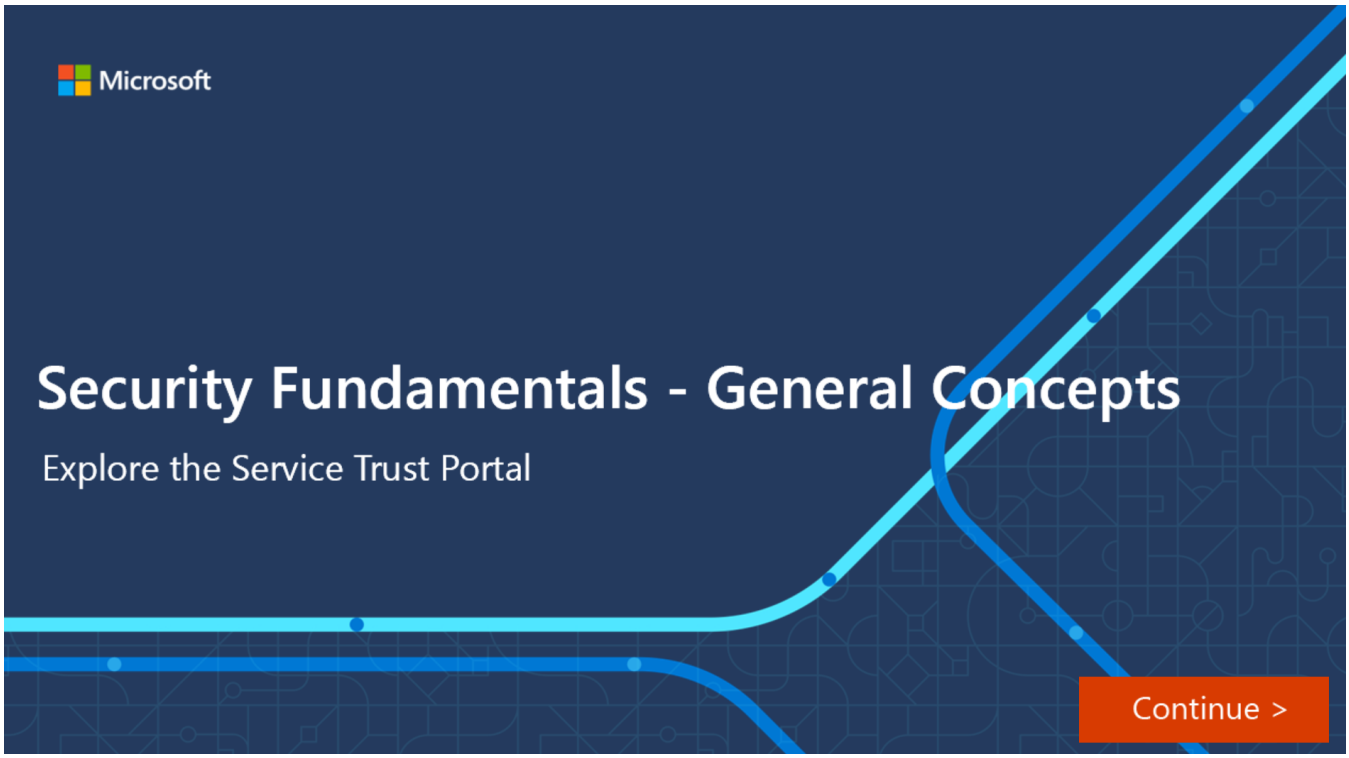
If a document is part of a series, you'll be subscribed to the series, and will receive notifications when there's an update to that series.



Interactive Guide

In this interactive guide, you'll explore a few of the menu options available on the Service Trust Portal. Select the image that follows to get started then follow the prompts on the screen.

> **Note**
>
> **The user interface (UI) in Microsoft 365 is continually evolving so the UI shown in the interactive guide may not reflect the most recent updates.**



Next unit: Describe Microsoft's privacy principles

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Describe Microsoft's privacy principles

4 minutes

Microsoft’s products and services run on trust. At Microsoft, we value, protect, and defend privacy. We believe in transparency, so that people and organizations can control their data and have meaningful choices in how it's used. We empower and defend the privacy choices of every person who uses our products and services.

Microsoft's approach to privacy is built on the following six principles:

- **Control: Putting you, the customer, in control of your data and your privacy with easy-to-use tools and clear choices. Your data is your business, and you can access, modify, or delete it at any time. Microsoft will not use your data without your agreement, and when we have your agreement, we use your data to provide only the services you have chosen. Your control over your data is reinforced by Microsoft compliance with broadly applicable privacy laws and privacy standards.**
- **Transparency: Being transparent about data collection and use so that everyone can make informed decisions. We only process your data based on your agreement and in accordance with the strict policies and procedures that we've contractually agreed to. When we deploy subcontractors or subprocessors to perform work that requires access to your data, they can perform only the functions that Microsoft has hired them to provide, and they're bound by the same contractual privacy commitments that Microsoft makes to you. The Microsoft Online Services Subprocessor List identifies authorized, subprocessors, who have been audited against a stringent set of security and privacy requirements in advance. This document is available as one of the data protection resources in the Service Trust Portal.**
- **Security: Protecting the data that's entrusted to Microsoft by using strong security and encryption. With state-of-the-art encryption, Microsoft protects your data both at rest and in transit. Our encryption protocols erect barriers against unauthorized access to the data, including two or more independent encryption layers to protect against compromises of any one layer. All Microsoft-managed encryption keys are properly secured and offer the use of technologies such as Azure Key Vault to help you control access to passwords, encryption keys, and other secrets.**
- **Strong legal protections: Respecting local privacy laws and fighting for legal protection of privacy as a fundamental human right. Microsoft defends your data through clearly defined and well-established response policies and processes, strong contractual commitments, and if necessary, the courts. We believe all**

government requests for your data should be directed to you. We don't give any government direct or unfettered access to customer data. We will not disclose data to a government or law enforcement agency, except as you direct or where required by law. Microsoft scrutinizes all government demands to ensure they're legally valid and appropriate. If Microsoft receives a request for your data, we'll promptly notify you and provide a copy of the request unless legally prohibited from doing so. Moreover, we'll direct the requesting party to seek the data directly from you. Our contractual commitments to our enterprise and public sector customers include defending your data, which builds on our existing protections. We'll challenge every government request for commercial and public sector customer data where we can lawfully do so.

- **No content-based targeting: Not using email, chat, files, or other personal content to target advertising. We do not share your data with advertiser-supported services, nor do we mine it for any purposes like marketing research or advertising.**
- **Benefits to you: When Microsoft does collect data, it's used to benefit you, the customer, and to make your experiences better. For example:**
  - **Troubleshooting: Troubleshooting for preventing, detecting, and repairing problems affecting operations of services.**
  - **Feature improvement: Ongoing improvement of features including increasing reliability and protection of services and data.**
  - **Personalized customer experience: Data is used to provide personalized improvements and better customer experiences.**

These principles form Microsoft's privacy foundation, and they shape the way that products and services are designed.

Next unit: Describe Microsoft Priva

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Describe Microsoft Priva

3 minutes

Privacy is top of mind for organizations and consumers today, and concerns about how private data is handled are steadily increasing. Regulations and laws impact people around the world, setting rules for how organizations store personal data and giving people rights to manage personal data collected by an organization.

To meet regulatory requirements and build customer trust, organizations need to take a "privacy by default" stance. Rather than manual processes and a patchwork of tools, organizations need a comprehensive solution to address common challenges such as:

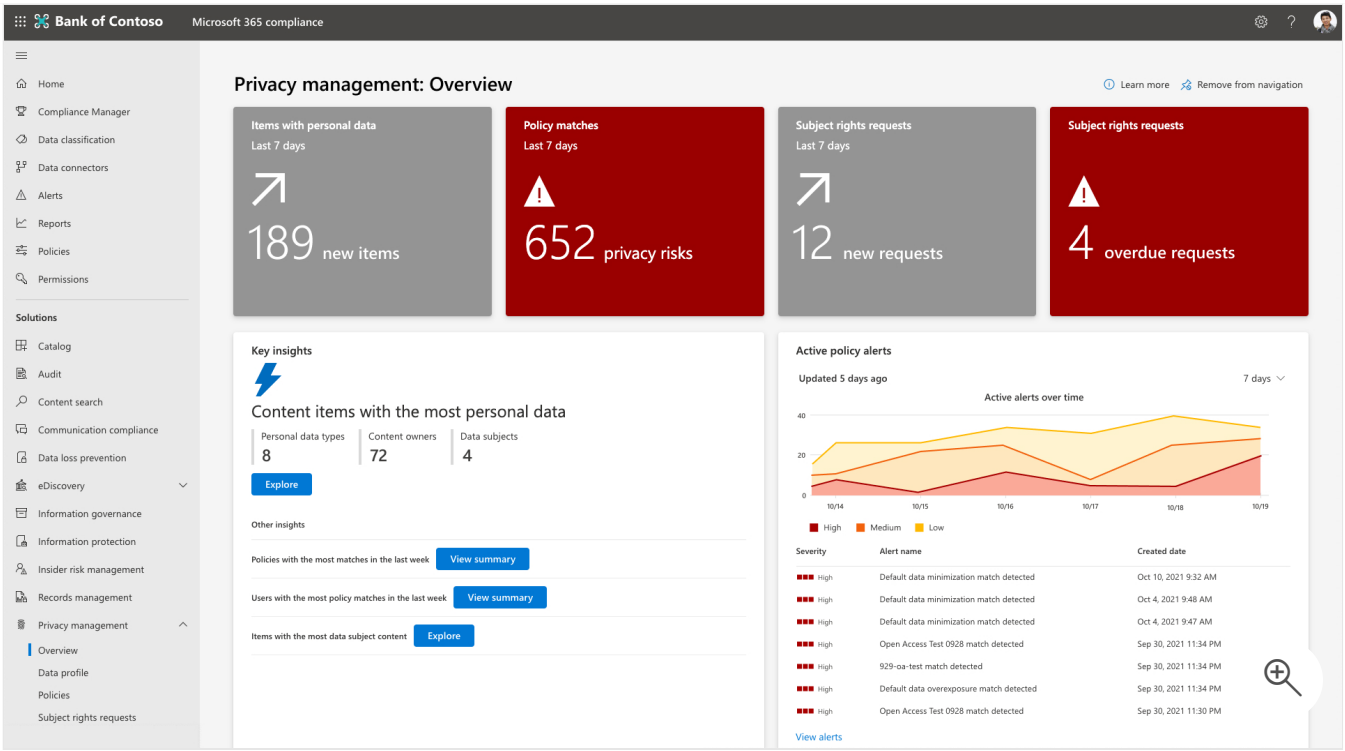
- **Helping employees adopt sound data handling practices and training them to spot and fix issues**
- **Understanding the potential risks in the amount and type of personal data they store and share**
- **Fulfilling data subject requests, or subject rights requests, efficiently and on-time**

Microsoft Priva helps you meet these challenges so you can achieve your privacy goals. Priva's capabilities are available through two solutions: Priva Privacy Risk Management, which provides visibility into your organization's data and policy templates for reducing risks; and Priva Subject Rights Requests, which provides automation and workflow tools for fulfilling data requests.

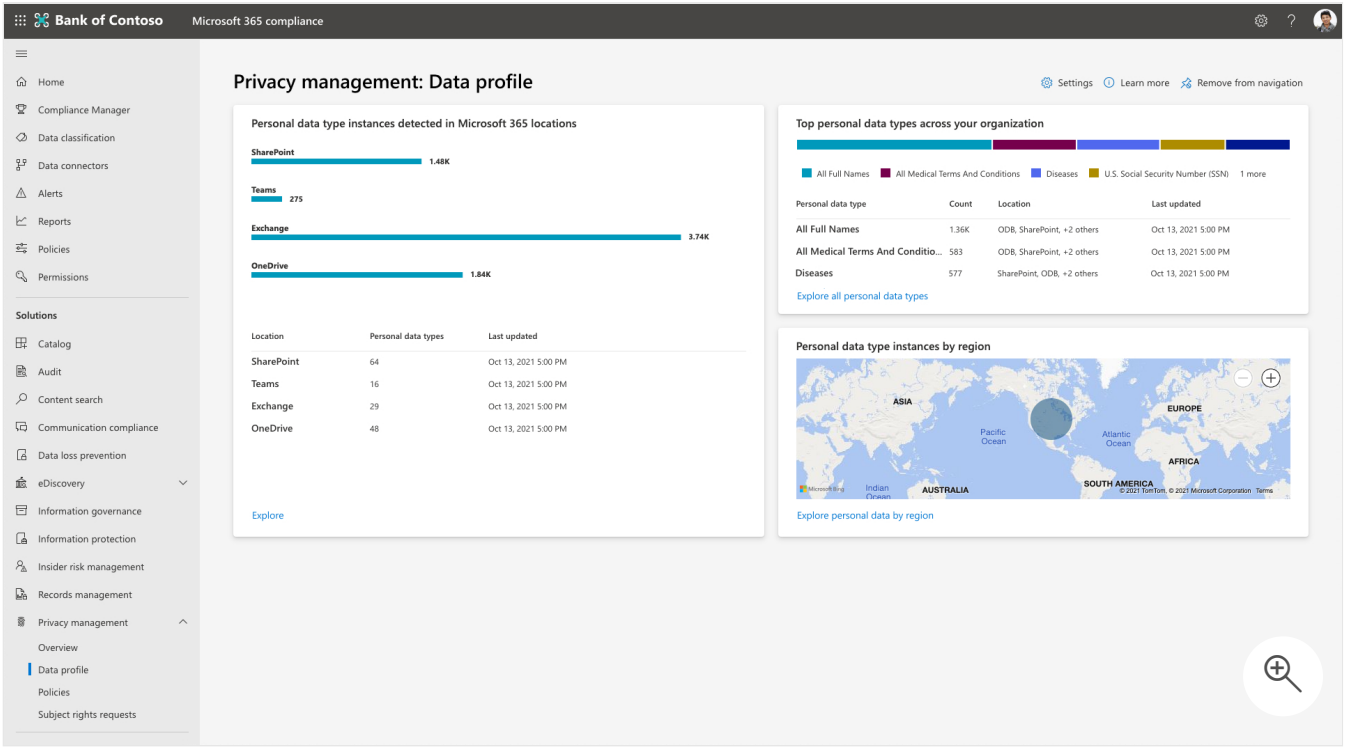
Priva Privacy Risk Management

Microsoft Priva helps you understand the data your organization stores by automating discovery of personal data assets and providing visualizations of essential information. These visualizations can be found on the overview and data profile pages, currently accessible through the Microsoft Purview compliance portal.

The overview dashboard provides an overall view into your organization’s data in Microsoft 365. Privacy administrators can monitor trends and activities, identify and investigate potential risks involving personal data, and springboard into key activities like policy management or subject rights request actions.



The data profile page in Priva provides a snapshot view of the personal data your organization stores in Microsoft 365 and where it lives. It also gives insight into the types of data you store.



Priva evaluates your organization's data stored in the following Microsoft 365 services within your Microsoft 365 tenant:

- **Exchange Online**
- **SharePoint Online**
- **OneDrive for Business**

- **Microsoft Teams**

Privacy Risk Management in Microsoft Priva also gives you the capability to set up policies that identify privacy risks in your Microsoft 365 environment and enable easy remediation. Privacy Risk Management policies are meant to be internal guides and can help you:

- **Detect overexposed personal data so that users can secure it.**
- **Spot and limit transfers of personal data across departments or regional borders.**
- **Help users identify and reduce the amount of unused personal data that you store.**

To learn more about Microsoft Priva Privacy Risk Management, select the interactive guide available in the Learn more section of the Summary and resources unit of this module.

Priva Subject Rights Requests

In accordance with certain privacy regulations around the world, individuals (or data subjects) may make requests to review or manage the personal data about themselves that companies have collected. These requests are sometimes also referred to as data subject requests (DSRs), data subject access requests (DSARs), or consumer rights requests. For companies that store large amounts of information, finding the relevant data can be a formidable task.

Microsoft Priva can help you handle these inquiries through the Subject Rights Requests solution. It provides workflow, automation, and collaboration capabilities for helping you search for subject data, review your findings, collect the appropriate files, and produce reports.

To learn more about Microsoft Priva Privacy Subject Rights Requests, select the interactive guide available in the Learn more section of the Summary and resources unit of this module.

Next unit: Knowledge check

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Summary and resources

1 minute

In this module, you learned about the Microsoft Service Trust Portal and the variety of content resources it provides about Microsoft security, privacy, and compliance practices. You learned about Microsoft's commitment to privacy and its privacy principles. Lastly, you learned about Microsoft Priva and how it helps organization's meet their privacy goals.

Now that you've completed this module, you should be able to:

- **Describe the offerings of the Service Trust Portal.**
- **Describe Microsoft's privacy principles.**
- **Describe Microsoft Priva.**

Learn more

- Service Trust Portal
- Get started with the Microsoft Service Trust Portal
- Trust Center
- Privacy at Microsoft
- Microsoft Privacy Statement
- Learn about Microsoft Priva
- Interactive guide - Microsoft Priva Privacy Risk Management
- Interactive guide - Microsoft Priva Subject Rights Requests

Module complete:

Unlock achievement

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Introduction

1 minute

Organizations must stay in line with compliance-related legal, regulatory, and privacy standards to protect their customers, partners, and themselves. Microsoft 365 provides tools and capabilities to enable organizations to manage compliance.

The Microsoft Purview compliance portal is the portal for organizations to manage their compliance needs using integrated solutions for information protection, data lifecycle management, insider risk management, auditing, and more.

In this module, you'll learn about the Microsoft Purview compliance portal. You'll learn about Compliance Manager and compliance score, which can help organizations manage, simplify, and improve compliance across their organization.

After completing this module, you'll be able to:

- **Describe the Microsoft Purview compliance portal.**
- **Describe Compliance Manager.**
- **Describe the use and benefits of compliance score.**

Next unit: Describe the Microsoft Purview compliance portal

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Describe the Microsoft Purview compliance portal

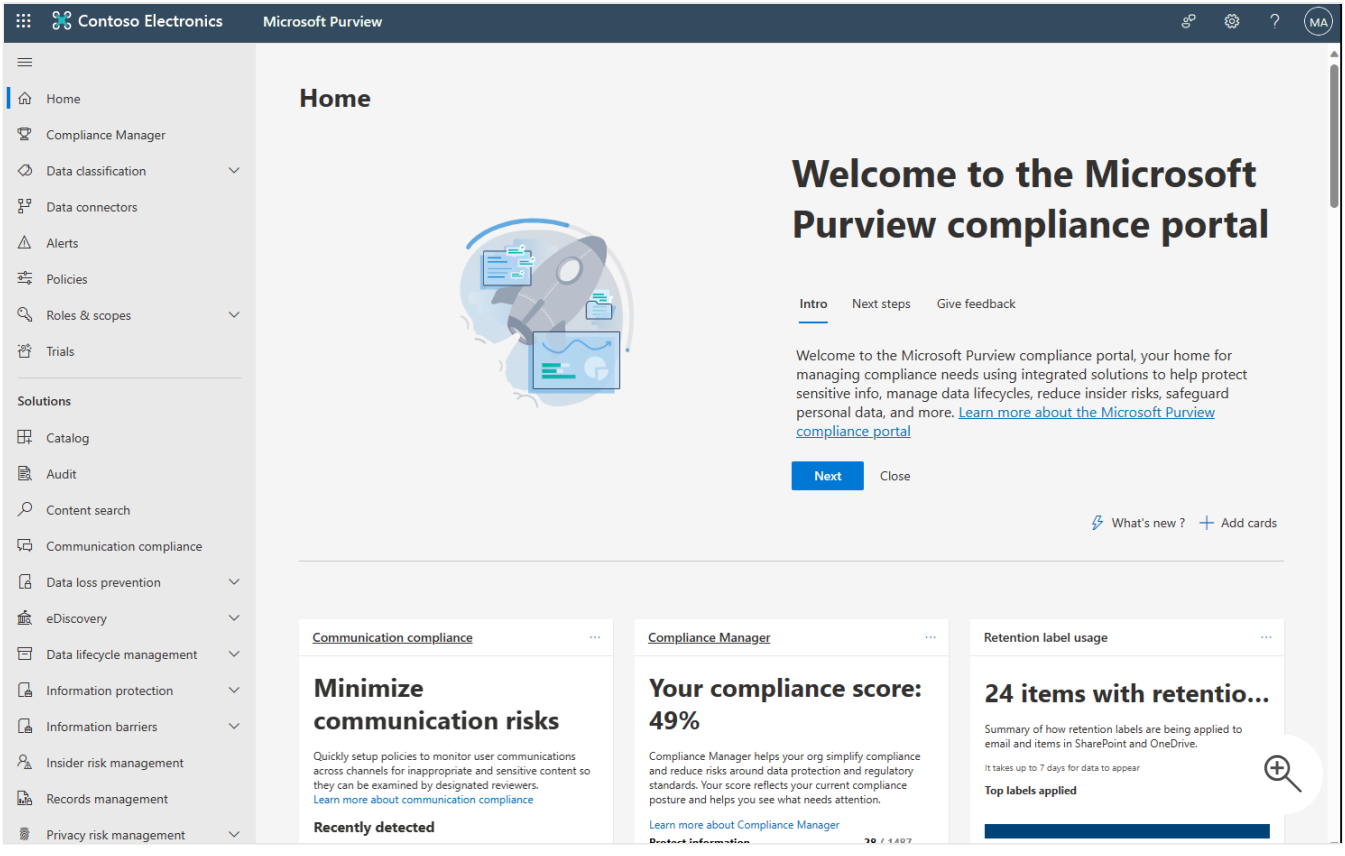
7 minutes

The Microsoft Purview compliance portal brings together all of the tools and data that are needed to help understand and manage an organization's compliance needs.

The compliance portal is available to customers with a Microsoft 365 SKU with one of the following roles:

- **Global administrator**
- **Compliance administrator**
- **Compliance data administrator**

When an admin signs in to the Microsoft Purview compliance portal, the card section on the home page shows, at a glance, how your organization is doing with data compliance, what solutions are available for your organization, and a summary of any active alerts. Admins can customize the card section by moving cards around or adding/removing cards that are displayed on the home screen.

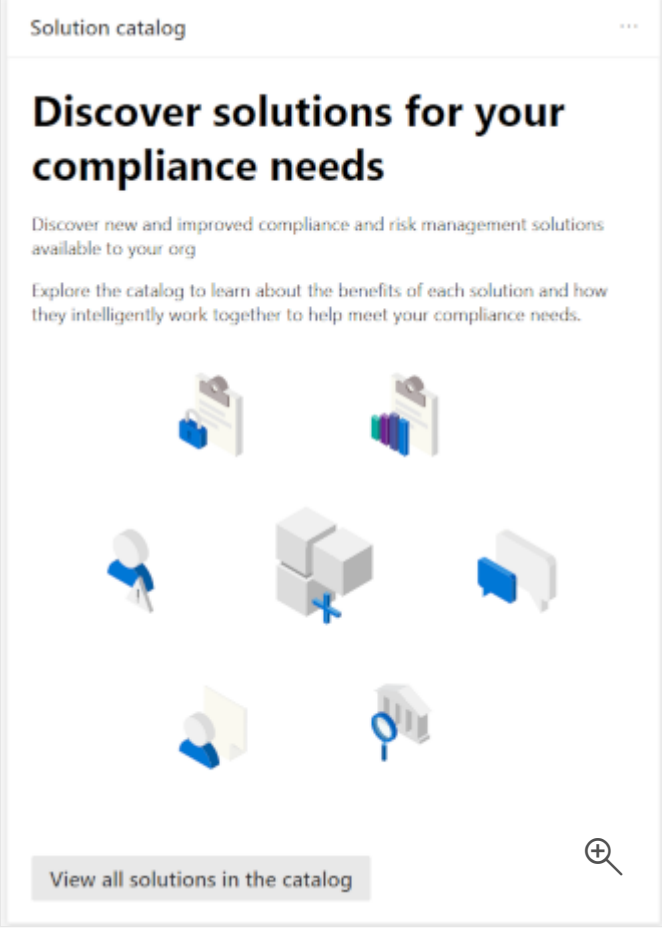


The default compliance portal home page contains several cards including:

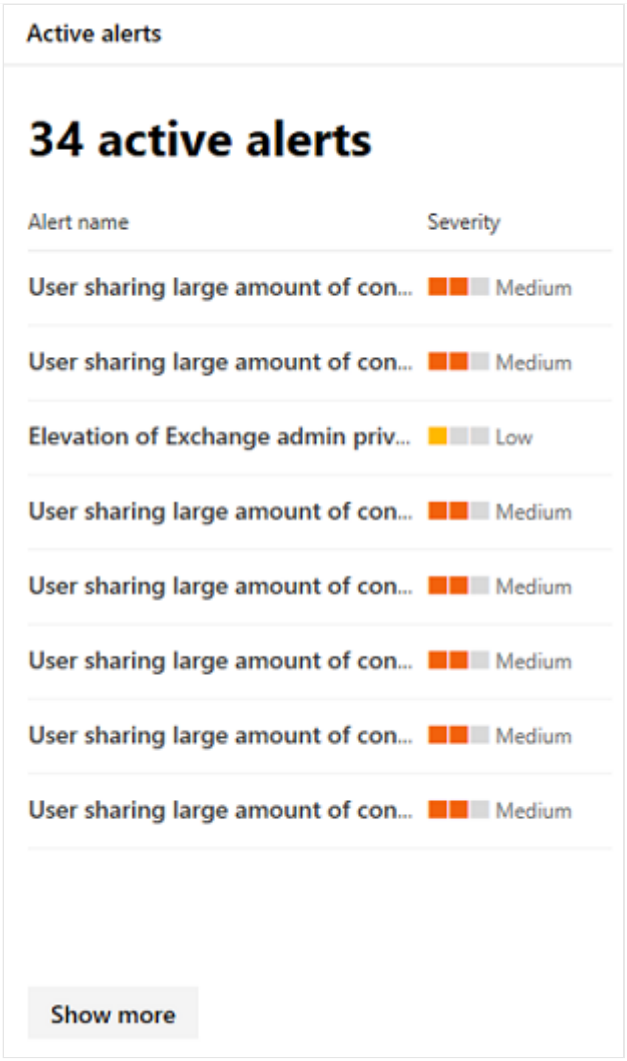
- **The Compliance Manager card. This card leads you to the Microsoft Purview Compliance Manager solution. Compliance Manager helps simplify the way you manage compliance. It calculates a risk-based compliance score that measures progress toward completing recommended actions to reduce risks associated with data protection and regulatory standards. The Compliance Manager solution also provides workflow capabilities and built-in control mapping to help you efficiently carry out improvement actions.**

- **The Solution catalog card links to collections of integrated solutions to help you manage end-to-end compliance scenarios. Solutions areas included:**
  - **Information protection & governance. These solutions help organizations classify, protect, and retain your data where it lives and wherever it goes. Included are data lifecycle management, data loss prevention, information protection, and records management.**

- **Privacy. Build a more privacy-resilient workplace. Privacy management gives actionable insights on your organization's personal data to help you spot issues and reduce risks.**
- **Insider risk management. These solutions help organizations identify, analyze, and remediate internal risks before they cause harm. Included are communication compliance, information barriers, and insider risk management.**
- **Discovery & response. These solutions help organizations quickly find, investigate, and respond with relevant data. Included are Audit, data subject requests, and eDiscovery.**

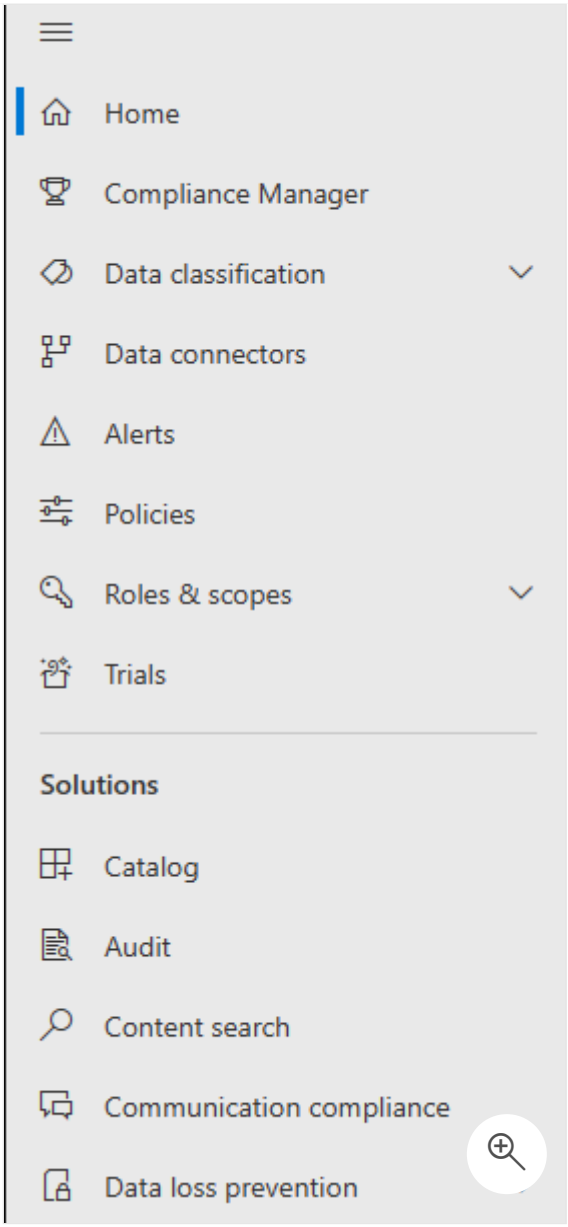


- **The Active alerts card includes a summary of the most active alerts and a link where admins can view more detailed information, such as alert severity, status, category, and more.**



Navigation

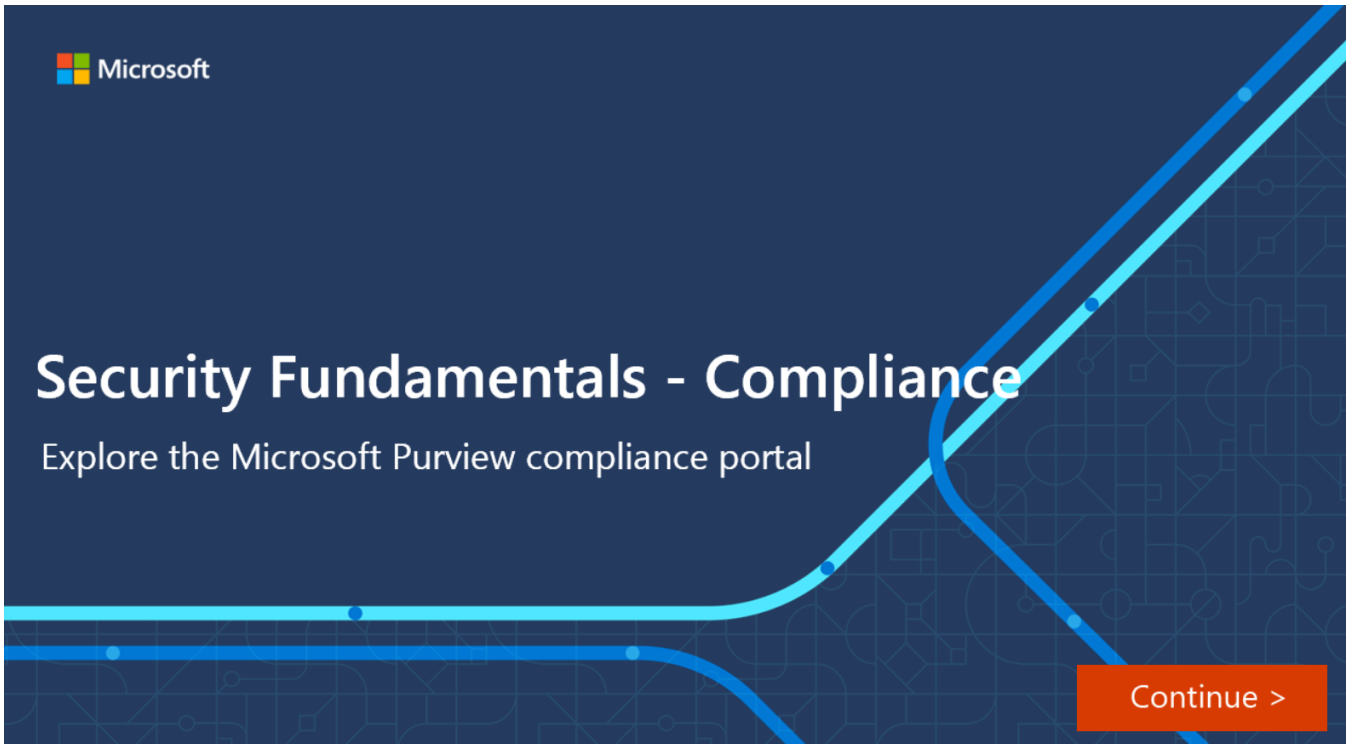
In addition to the cards on the home page, there's a navigation pane on the left of the screen that gives easy access to the Compliance Manager and the Data Classification page where you can get snapshots of how sensitive information and labels are being used across your organization's locations. You can access alerts, reports, policies, and all the solutions that are included in the solutions catalog. There's access to data connectors that you can use to import non-Microsoft data to Microsoft 365 so it can be covered by your compliance solutions. The Customize navigation control allows customization of which items appear in the navigation pane.



Interactive guide

In this interactive guide, you'll explore some of the capabilities of the Microsoft Purview compliance portal, your home for managing compliance needs using integrated solutions for information protection, data lifecycle management, insider risk management, discovery, and more. Select the image that follows to get started and follow the prompts on the screen.

> **Note**
>
> **The user interface (UI) in Microsoft 365 is continually evolving so the UI shown in the interactive guide may not reflect the most recent updates.**



Next unit: Describe Compliance Manager

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Describe Compliance Manager

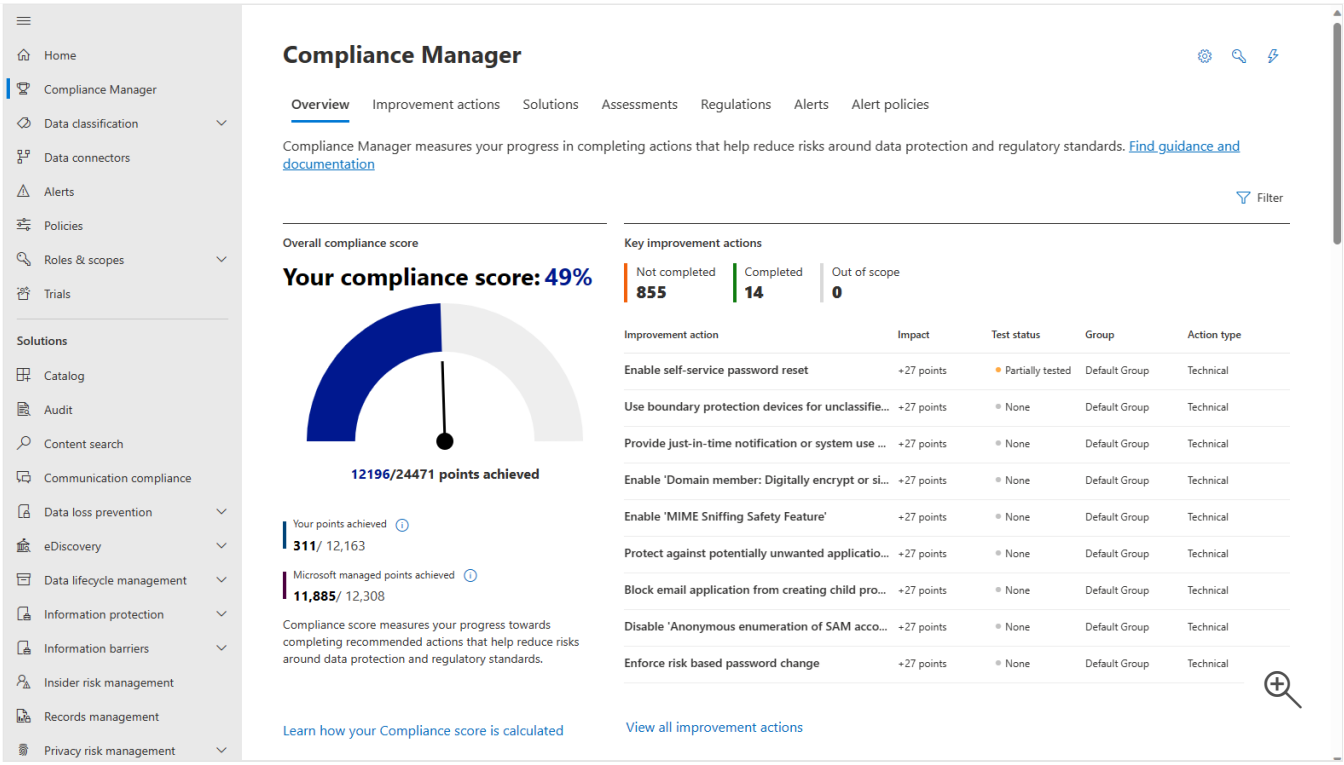
10 minutes

Microsoft Purview Compliance Manager is a feature in the Microsoft Purview compliance portal that helps admins to manage an organization's compliance requirements with greater ease and convenience. Compliance Manager can help organizations throughout their compliance journey, from taking inventory of data protection risks, to managing the complexities of implementing controls, staying current with regulations and certifications, and reporting to auditors.

Compliance Manager helps simplify compliance and reduce risk by providing:

- **Prebuilt assessments based on common regional and industry regulations and standards. Admins can also use custom assessment to help with compliance needs unique to the organization.**
- **Workflow capabilities that enable admins to efficiently complete risk assessments for the organization.**
- **Step-by-step improvement actions that admins can take to help meet regulations and standards relevant to the organization. Some actions will also be managed for the organization by Microsoft. Admins will get implementation details and audit results for those actions.**
- **Compliance score, which is a calculation that helps an organization understand its overall compliance posture by measuring how it's progressing with improvement actions.**

The Compliance Manager dashboard shows the current compliance score, helps admins to see what needs attention, and guides them to key improvement actions.



Compliance Manager uses several data elements to help manage compliance activities. As admins use Compliance Manager to assign, test, and monitor compliance activities, it's helpful to have a basic understanding of the key elements: controls, assessments, templates, and improvement actions.

Controls

A control is a requirement of a regulation, standard, or policy. It defines how to assess and manage system configuration, organizational process, and people responsible for meeting a specific requirement of a regulation, standard, or policy.

Compliance Manager tracks the following types of controls:

- **Microsoft-managed controls: controls for Microsoft cloud services, which Microsoft is responsible for implementing.**
- **Your controls: sometimes referred to as customer-managed controls, these are implemented and managed by the organization.**
- **Shared controls: responsibility for implementing these controls is shared by the organization and Microsoft.**

Compliance Manager continuously assesses controls by scanning through your Microsoft 365 environment and detecting your system settings, continuously and automatically updating your technical action status.

Assessments

An assessment is a grouping of controls from a specific regulation, standard, or policy. Completing the actions within an assessment helps to meet the requirements of a standard, regulation, or law. For example, an organization may have an assessment that, when completed, helps to bring the organization's Microsoft 365 settings in line with ISO 27001 requirements.

An assessment consists of several components including the services that are in-scope, the Microsoft managed controls, your controls, shared controls, and an assessment score that shows progress towards completing the actions needed for compliance.

Templates

Compliance Manager provides templates to help admins to quickly create assessments. They can modify these templates to create an assessment optimized for their needs. Admins can also build a custom assessment by creating a template with their own controls and actions. For example, the admin may want a template to cover an internal business process control, or a regional data protection standard that isn't covered by one of Microsoft's 150-plus prebuilt assessment templates.

Improvement actions

Improvement actions help centralize compliance activities. Each improvement action provides recommended guidance that's intended to help organizations to align with data protection regulations and standards. Improvement actions can be assigned to users in the organization to do implementation and testing work. Admins can also store documentation, notes, and record status updates within the improvement action.

Benefits of Compliance Manager

Compliance Manager provides many benefits, including:

- **Translating complicated regulations, standards, company policies, or other control frameworks into a simple language.**
- **Providing access to a large variety of out-of-the-box assessments and custom assessments to help organizations with their unique compliance needs.**
- **Mapping regulatory controls against recommended improvement actions.**
- **Providing step-by-step guidance on how to implement the solutions to meet regulatory requirements.**
- **Helping admins and users to prioritize actions that will have the highest impact on their organizational compliance by associating a score with each action.**

Interactive guide

In this interactive guide, you'll explore Compliance Manager. Select the image that follows to get started and follow the prompts on the screen.

Next unit: Describe use and benefits of compliance score

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

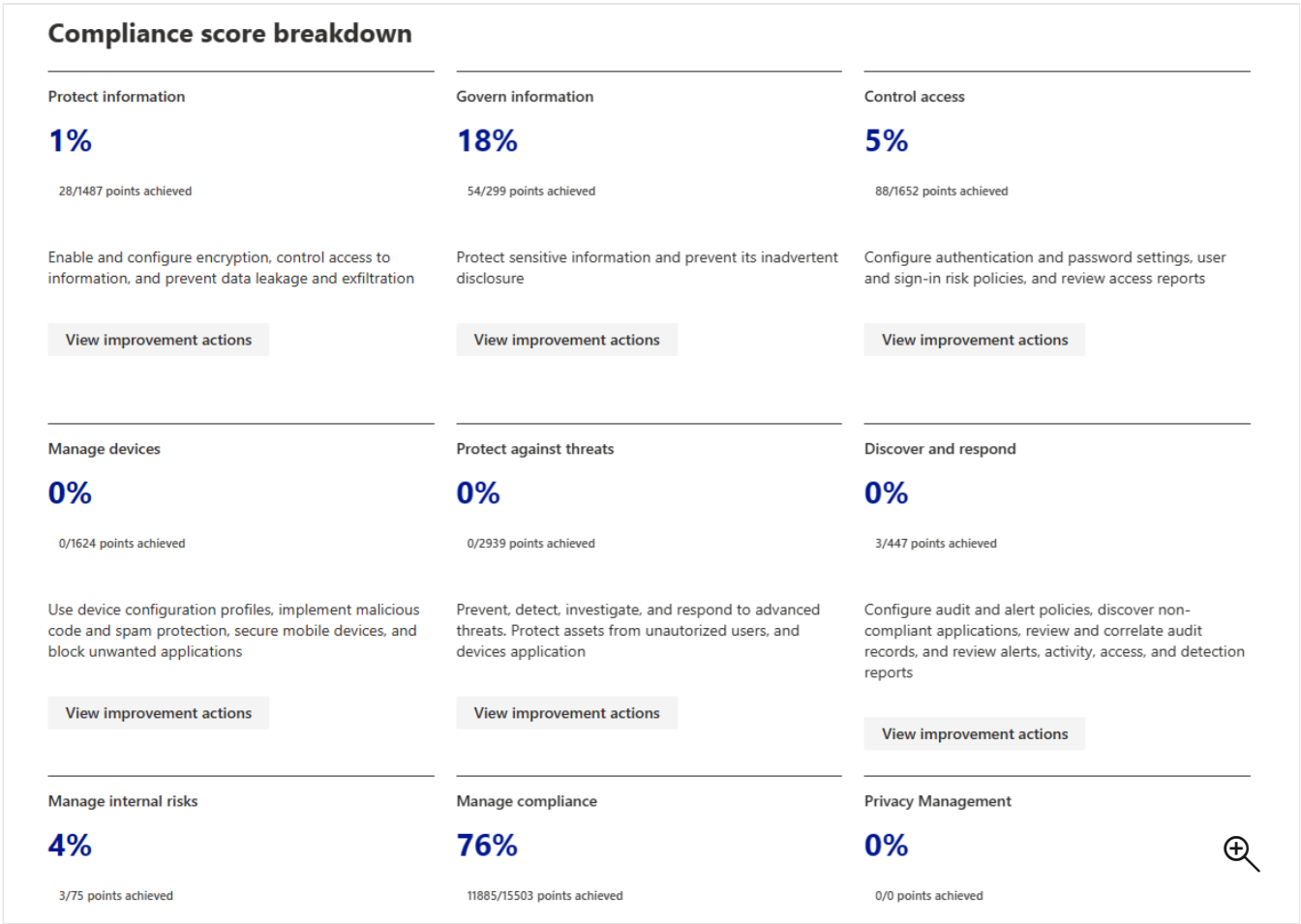
100 XP

Describe use and benefits of compliance score

3 minutes

Compliance score measures progress in completing recommended improvement actions within controls. The score can help an organization to understand its current compliance posture. It also helps organizations to prioritize actions based on their potential to reduce risk.

Admins can get a breakdown of the compliance score in the Compliance Manager overview pane.



How to understand the compliance score

The overall compliance score is calculated using scores that are assigned to actions. Actions come in two types:

- **Your improved actions: actions that the organization is expected to manage.**
- **Microsoft actions: actions that Microsoft manages for the organization.**

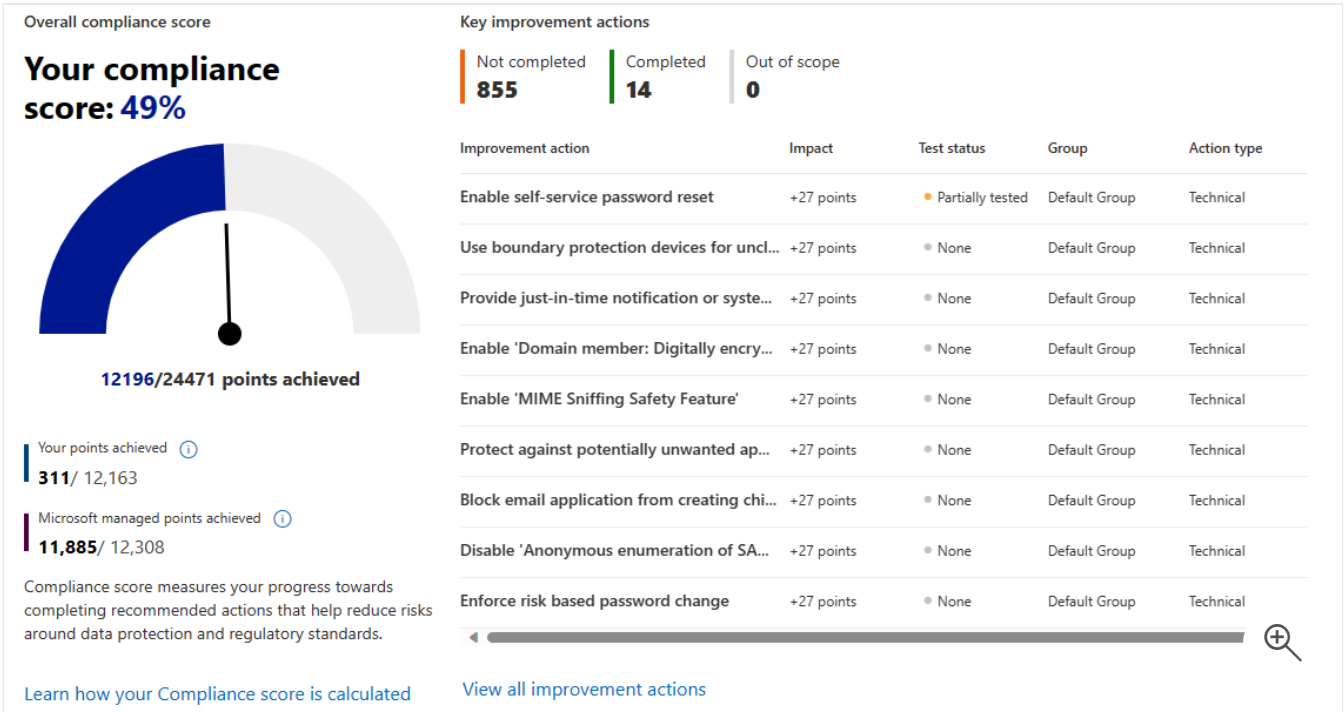
Actions are categorized as mandatory, discretionary, preventative, detective, or corrective:

- **Mandatory – these actions shouldn't be bypassed. For example, creating a policy to set requirements for password length or expiration.**
- **Discretionary – these actions depend on the users understanding and adhering to a policy. For example, a policy where users are required to ensure their devices are locked before they leave them.**

The following are subcategories of actions that can be classified as mandatory or discretionary:

- **Preventative actions are designed to handle specific risks, like using encryption to protect data at rest if there were breaches or attacks.**
- **Detective actions actively monitor systems to identify irregularities that could represent risks, or that can be used to detect breaches or intrusions. Examples of these types of actions are system access audits, or regulatory compliance audits.**
- **Corrective actions help admins to minimize the adverse effects of security incidents, by undertaking corrective measures to reduce their immediate effect or possibly even reverse damage.**

Organizations accumulate points for every action completed. And the compliance score is shown as a percentage representing all the actions completed, compared with the ones outstanding.



What is the difference between Compliance Manager and compliance score?

Compliance Manager is an end-to-end solution in the Microsoft Purview compliance portal to enable admins to manage and track compliance activities. Compliance score is a calculation of the overall compliance posture across the organization. The compliance score is available through Compliance Manager.

Compliance Manager gives admins the capabilities to understand and increase their compliance score, so they can ultimately improve the organization's compliance posture and help it to stay in line with compliance requirements.

Next unit: Knowledge check

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Summary and resources

1 minute

You've learned about the various tools provided by Microsoft Purview to manage compliance for your organization. You explored the compliance portal, which enables organizations to manage their compliance needs. You learned how Compliance Manager and compliance score can help organizations manage, simplify, and improve compliance across their organization.

Now that you've completed this module, you should be able to:

- **Describe the Microsoft Purview compliance portal.**
- **Describe Compliance Manager.**
- **Describe the use and benefits of compliance score.**

Learn more

- Microsoft Purview compliance portal
- Microsoft Purview Compliance Manager
- Compliance score calculation
- Compliance Manager frequently asked questions

Explore other modules

Microsoft Security, Compliance, and Identity Fundamentals: Describe the capabilities of Microsoft compliance solutions
MS-900 Microsoft 365 Fundamentals: Describe Microsoft 365 security and compliance capabilities

100 XP

Introduction

1 minute

Organizations need to protect all sorts of information, including financial and personal information. This must be done to ensure customers, employees, and the organization are protected from risks. The organization needs to stay in line with compliance standards wherever it operates.

Information protection and data lifecycle management in Microsoft Purview helps organizations classify, protect, and retain their data where it lives and wherever it goes.

In this module, you'll learn about how Microsoft Purview solutions and capabilities like data classification, records management, and data loss prevention, can help organizations with their information protection and data lifecycle management needs.

After completing this module, you'll be able to:

- **Describe data classification capabilities.**
- **Describe data loss prevention.**
- **Describe records management.**

Next unit: Know your data, protect your data, and govern your data

Continue

100 XP

Know your data, protect your data, and govern your data

2 minutes

Microsoft Purview Information Protection discovers, classifies, and protects sensitive and business-critical content throughout its lifecycle across your organization. It provides the tools to know your data, protect your data, and prevent data loss.

Microsoft Purview Data Lifecycle Management manages your content lifecycle using solutions to import, store, and classify business-critical data so you can keep what you need and delete what you don't. It gives organizations the capabilities to govern their data, for compliance or regulatory requirements.

Information protection and data lifecycle management work together to classify, protect, and govern your data where it lives, and wherever it goes.

- **Know your data: Organizations can understand their data landscape and identify important data across on-premises, cloud, and hybrid environments. Capabilities and tools such as trainable classifiers, activity explorer, and content explorer allow organizations to know their data.**
- **Protect your data: Organizations can apply flexible protection actions including encryption, access restrictions, and visual markings.**
- **Prevent data loss: Organizations can detect risky behavior and prevent accidental oversharing of sensitive information. Capabilities such as data loss prevention policies and endpoint data loss prevention enable organizations to avoid data loss.**
- **Govern your data: Organizations can automatically keep, delete, and store data and records in a compliant manner. Data lifecycle management capabilities, like**

retention policies, retention labels, and records management enable organizations to govern their data.

Next unit: Describe the data classification capabilities of the compliance portal

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Describe the data classification capabilities of the compliance portal

11 minutes

Organizations need to know their data to identify important information across the estate and ensure that data is handled in line with compliance requirements. Admins can enable their organization to know its data through data classification capabilities and tools in the Microsoft Purview compliance portal, such as sensitive information types, trainable classifiers, content explorer, and activity explorer.

Identifying and classifying sensitive items that are under your organization's control is the first step in the Information Protection discipline. Microsoft Purview provides three ways of identifying items so that they can be classified:

- **manually by users**
- **automated pattern recognition, like sensitive information types**
- **machine learning**

Sensitive information types

Sensitive information types (SIT) are pattern-based classifiers. They have set patterns that can be used to identify them. For example, an identification number in a country/region may be based on a specific pattern, like this:

123-456-789-ABC

Microsoft Purview includes many built-in sensitive information types based on patterns that are defined by a regular expression (regex) or a function.

Examples include:

- **Credit card numbers**
- **Passport or identification numbers**
- **Bank account numbers**
- **Health service numbers**

Refer to Sensitive information type entity definitions for a listing of available built-in sensitive information types.

Data classification in Microsoft Purview also supports the ability to create custom sensitive information types to address organization-specific requirements. For example, an organization may need to create sensitive information types to represent employee IDs or project numbers.

Also supported is exact data match (EDM) classification. EDM-based classification enables you to create custom sensitive information types that refer to exact values in a database of sensitive information.

To explore how to classify data using sensitive info types with Microsoft Purview Information Protection, select the interactive guide available in the Learn more section of the Summary and resources unit of this module.

Trainable classifiers

Trainable classifiers use artificial intelligence and machine learning to intelligently classify your data. They're most useful classifying data unique to an organization like specific kinds of contracts, invoices, or customer records. This method of classification is more about training a classifier to identify an item based on what the item is, not by elements that are in the item (pattern matching). Two types of classifier are available:

- **Pre-trained classifiers - Microsoft has created and pretrained many classifiers that you can start using without training them. These classifiers will appear with the status of Ready to use. Microsoft Purview comes with five pretrained classifiers that detect and classify things like resumes, source code, harassment, profanity, and threat (relates to committing violence or doing physical harm).**
- **Custom trainable classifiers - Microsoft supports the ability to create and train custom classifiers. They're most useful when classifying data unique to an organization, like specific kinds of contracts, invoices, or customer records.**

To get a custom trainable classifier to accurately identify an item as being in a particular category of content, it must first be presented with many samples of the type of content in the category. This feeding of positive samples is known as seeding and is used to create a prediction model for the classifier.

The model gets tested to determine if the classifier can correctly distinguish between items that match the category and items that don't. The result of each prediction is manually verified, which serves as input to improve the accuracy of the prediction model.

After the accuracy score of the model has stabilized, the classifier can be published. Trainable classifiers can then sort through items in locations like SharePoint Online,

Exchange, and OneDrive, and classify the content.

> **Note**
>
> **At this time, classifiers only work with items that aren't encrypted.**

Understand and explore the data

Data classification can involve large numbers of documents and emails. To help administrators to easily derive insights and understanding, the overview section of the data classification pane in compliance portal provides many details at a glance, including:

- **The number of items classified as sensitive information and which classifications they are.**
- **Details on the locations of data based on sensitivity.**
- **Summary of actions that users are taking on sensitive content across the organization.**

Administrators can also use the content and activity explorers to gain a deeper understanding and guide their actions.

What is the content explorer?

The content explorer is available as a tab in the data classification pane of compliance portal. It enables administrators to gain visibility into the content that has been summarized in the overview pane.

Access to content explorer is highly restricted because it makes it possible to read the contents of scanned files. There are two roles that grant access to content explorer:

- **Content explorer list viewer.**
- **Content explorer content viewer.**

Anyone who wants to access content explorer must have an account in one or both of the role groups.

With content explorer, administrators get a current snapshot of individual items that have been classified across the organization. It enables administrators to further drill down into items by allowing them to access and review the scanned source content that's stored in different kinds of locations, such as Exchange, SharePoint, and OneDrive.

What is the activity explorer?

Activity explorer provides visibility into what content has been discovered and labeled, and where that content is. It makes it possible to monitor what's being done with labeled content across the organization. Admins gain visibility into document-level activities like label changes and label downgrades (such as when someone changes a label from confidential to public).

Admins use the filters to see all the details for a specific label, including file types, users, and activities. Activity explorer helps you understand what's being done with labeled content over time. Admins use activity explorer to evaluate if controls already in place are effective.

Here are a few of the activity types that can be analyzed:

- **File copied to removable media**
- **File copied to network share**
- **Label applied**
- **Label changed**

Admins can use more than 30 filters for data including:

- **Location**
- **User**
- **Sensitivity label**
- **Retention label**

The value of understanding what actions are being taken with sensitive content is that admins can see if the controls that they've already put in place, such as data loss prevention policies, are effective or not. For example, if it's discovered that a large number of items labeled *Highly Confidential* have suddenly been downgraded to *Public*, admins can update policies and act to restrict undesired behavior as a response.

Explore data classification in the compliance portal

The video below walks you through the various data classification capabilities available in the compliance portal.

> **Note**

The user interface (UI) in Microsoft 365 is continually evolving so the UI shown in the video may not reflect the most recent updates.

Next unit: Describe sensitivity labels and policies

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Describe sensitivity labels and policies

5 minutes

Organizations must protect their data, to safeguard customers and business operations, and to meet compliance standards. Admins can enable their organization to protect its data, through capabilities and tools such as sensitivity labels and policies in the Microsoft Purview compliance portal.

Sensitivity labels

Sensitivity labels, available as part of information protection in the Microsoft Purview compliance portal, enable the labeling and protection of content, without affecting productivity and collaboration. With sensitivity labels, organizations can decide on labels to apply to content such as emails and documents, much like different stamps are applied to physical documents:

Labels are:

- **Customizable: Admins can create different categories specific to the organization, such as Personal, Public, Confidential, and Highly Confidential.**
- **Clear text: Because each label is stored in clear text in the content's metadata, third-party apps and services can read it and then apply their own protective actions, if necessary.**
- **Persistent. After you apply a sensitivity label to content, the label is stored in the metadata of that email or document. The label then moves with the content, including the protection settings, and this data becomes the basis for applying and enforcing policies.**

Each item that supports sensitivity labels can only have one label applied to it, at any given time.

Sensitivity labels can be configured to:

- **Encrypt email only or both email and documents.**
- **Mark the content when Office apps are used. Marking the content includes adding watermarks, headers, or footers. Headers or footers can be added to emails or documents. Watermarks can be applied to documents but not to email.**
- **Apply the label automatically in Office apps or recommend a label. Admins choose the types of sensitive information to be labeled. The label can be applied**

automatically or configured to prompt users to apply the recommended label.

- Protect content in containers such as sites and groups. This label configuration doesn't result in documents being automatically labeled. Instead, the label settings protect content by controlling access to the container where documents are stored.
- Extend sensitivity labels to third-party apps and services. The Microsoft Purview Information Protection SDK enables third-party apps to read sensitivity labels and apply protection settings.
- Classify content without using any protection settings. A classification can be assigned to content (just like a sticker) that persists and roams with the content as it's used and shared. The classification can be used to generate usage reports and view activity data for sensitive content.

Label policies

After sensitivity labels are created, they need to be published to make them available to people and services in the organization. Sensitivity labels are published to users or groups through label policies. Sensitivity labels will then appear in Office apps for those users and groups. The sensitivity labels can be applied to documents and emails. Label policies enable admins to:

- Choose the users and groups that can see labels. Labels can be published to specific users, distribution groups, Microsoft 365 groups in Azure Active Directory, and more.
- Apply a default label to all new emails and documents that the specified users and groups create. Users can always change the default label if they believe the document or email has been mislabeled.
- Require justifications for label changes. If a user wants to remove a label or replace it, admins can require the user to provide a valid justification to complete the action. The user will be prompted to provide an explanation for why the label should be changed.
- Require users to apply a label (mandatory labeling). It ensures a label is applied before users can save their documents, send emails, or create new sites or groups.
- Link users to custom help pages. It helps users to understand what the different labels mean and how they should be used.

Once a sensitivity label is applied to an email or document, any configured protection settings for that label are enforced on the content.

To learn more, explore the interactive guides available in the Learn more section of the Summary and resources unit of this module.

Next unit: Describe data loss prevention

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Describe data loss prevention

5 minutes

Data loss can harm an organization's customers, business processes, and the organization itself. Organizations need to prevent data loss by detecting risky behavior and preventing sensitive information from being shared inappropriately. Admins can use data loss prevention policies, available in the Microsoft Purview compliance portal, to help their organization.

Microsoft Purview Data Loss Prevention (DLP) is a way to protect sensitive information and prevent its inadvertent disclosure. With DLP policies, admins can:

- **Identify, monitor, and automatically protect sensitive information across Microsoft 365, including:**
  - **OneDrive for Business**
  - **SharePoint Online**
  - **Microsoft Teams**
  - **Exchange Online**
- **Help users learn how compliance works without interrupting their workflow. For example, if a user tries to share a document containing sensitive information, a DLP policy can send them an email notification and show them a policy tip.**
- **View DLP reports showing content that matches the organization's DLP policies. To assess how the organization is following a DLP policy, admins can see how many matches each policy has over time.**

DLP policies protect content through the enforcement of rules that consist of:

- **Conditions that the content must match before the rule is enforced.**
- **Actions that the admin wants the rule to take automatically when content that matches the conditions has been found.**
- **Locations where the policy will be applied, such as Exchange, SharePoint, OneDrive, and more.**

For example, an admin can configure a DLP policy that helps detect information that's subject to a compliance regulation like the Health Insurance Portability and Accountability Act (HIPAA) across all SharePoint sites and OneDrive for Business. The admin can block the relevant documents from being shared inappropriately.

DLP policies protect information by identifying and automatically protecting sensitive data. Here's some scenarios where DLP policies can help:

- **Identify any document containing a credit card number stored in users' OneDrive for Business accounts.**
- **Automatically block an email containing employee personal information from being sent outside the organization.**

A policy can contain one or more rules, and each rule consists of conditions and actions at a minimum. For each rule, when the conditions are met, the actions are taken automatically. Rules can be grouped into one policy, to help simplify management and reporting. The diagram below shows how multiple rules, each with their own conditions and actions, are grouped into a single policy.

The rules inside the policy are prioritized in how they're implemented. For example, in the above diagram, rule one will be prioritized before rule two, and so on.

What is endpoint data loss prevention?

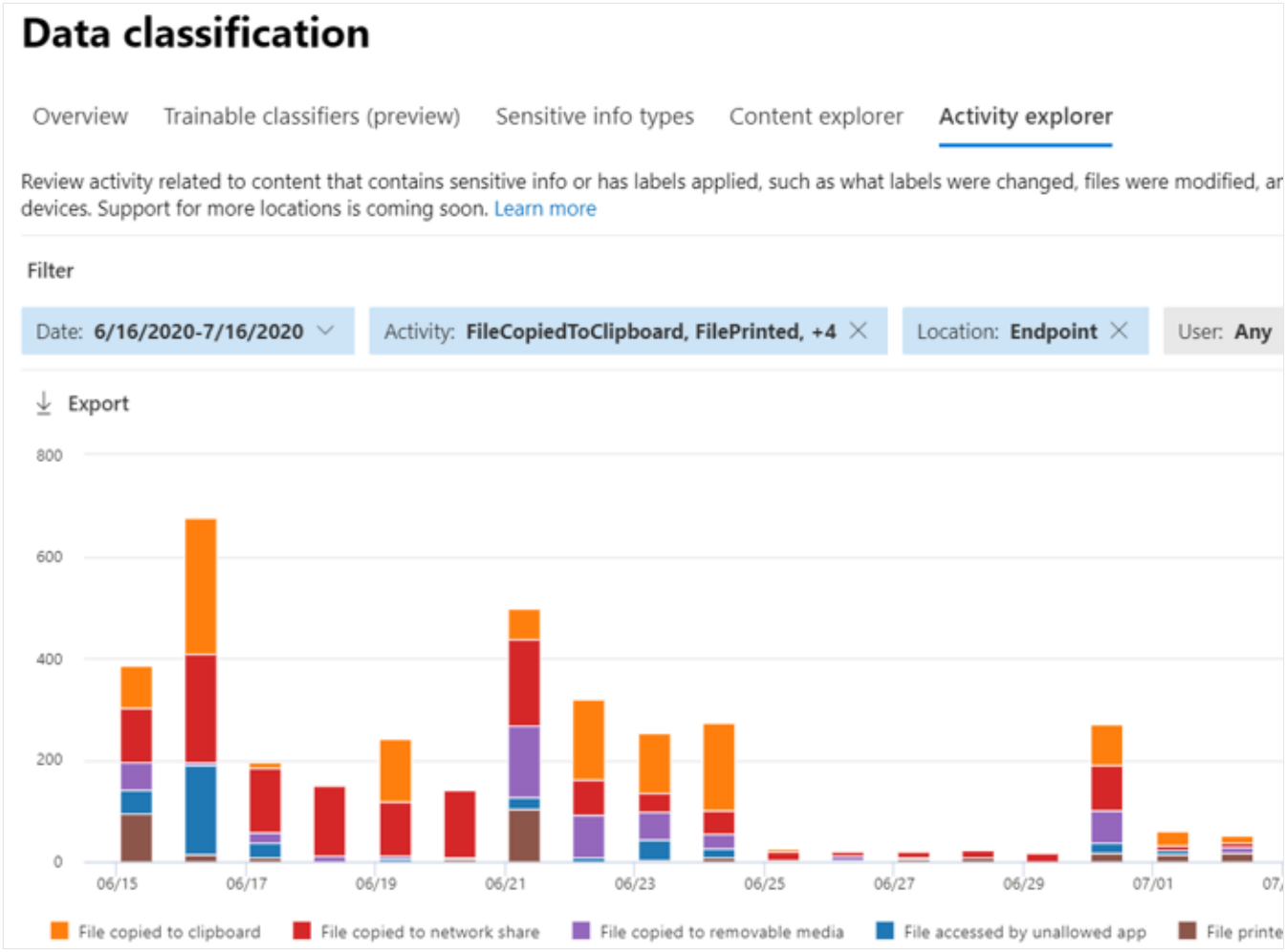
Endpoint data loss prevention (Endpoint DLP) extends the activity monitoring and protection capabilities of DLP to sensitive items that are physically stored on Windows 10, Windows 11, and macOS (Catalina 10.15 and higher) devices

Endpoint DLP enables admins to audit and manage activities that users complete on sensitive content. Listed below are a few examples:

- **Creating an item**
- **Renaming an item**

- **Copying items to removable media**
- **Copying items to network shares**
- **Printing documents**
- **Accessing items using unallowed apps and browsers**

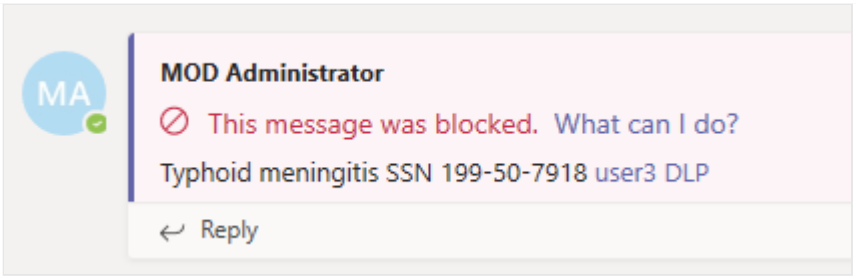
In the activity explorer, you can view information about what users are doing with sensitive content.



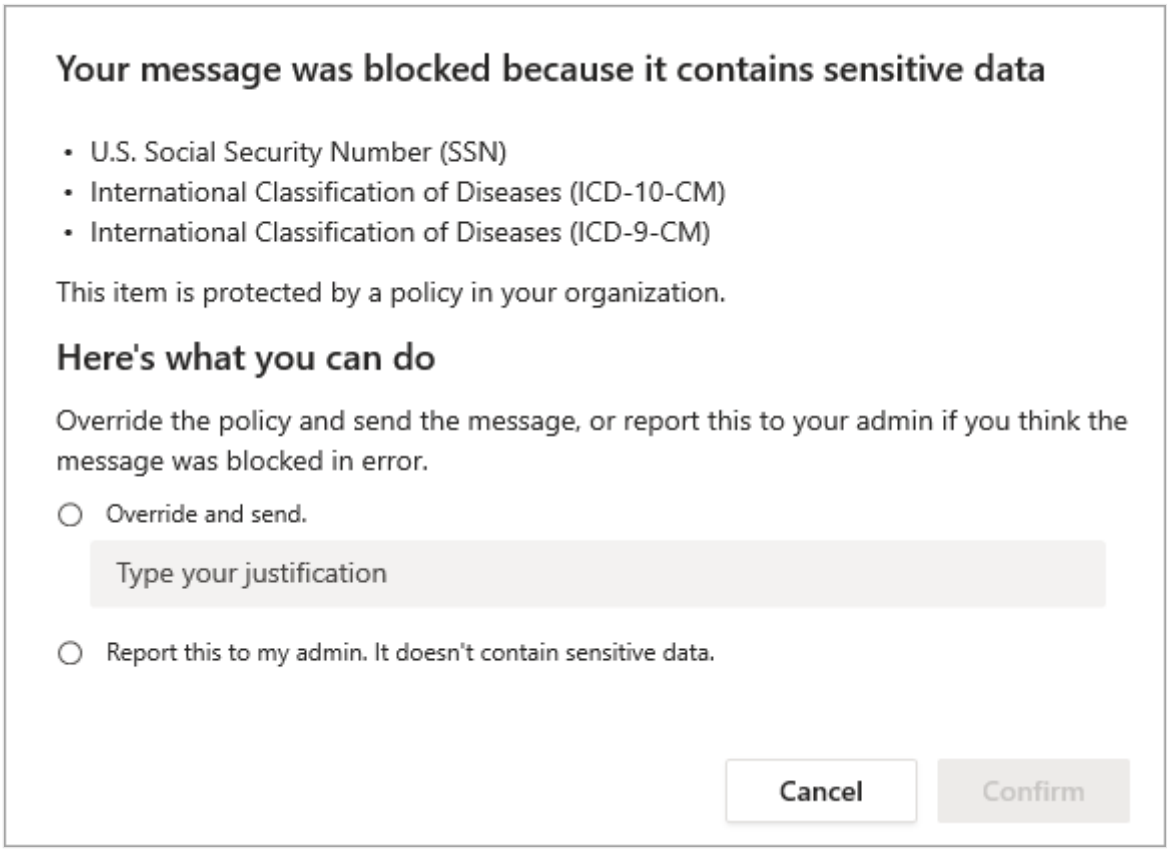
Admins use this information to enforce protective actions for content through controls and policies.

Data loss prevention in Microsoft Teams

Data loss prevention capabilities have been extended to Microsoft Teams chat and channel messages, including messages in private channels. With DLP, administrators can now define policies that prevent users from sharing sensitive information in a Teams chat session or channel, whether it's in a message, or a file. Just like with Exchange, Outlook, SharePoint, and OneDrive for Business, administrators can use DLP policy tips that will be displayed to the user to show them why a policy has been triggered. For example, the screenshot below shows a policy tip on a chat message that was blocked because the user attempted to share a U.S. Social Security Number.



The user can then find out more about why their message was blocked by selecting the "What can I do?" link, and take appropriate action.



With DLP policies, Microsoft Teams can help users across organizations to collaborate securely and in a way that's in line with compliance requirements.

Next unit: Describe retention policies and retention labels

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Describe retention policies and retention labels

3 minutes

Retention labels and policies help organizations to manage and govern information by ensuring content is kept only for a required time, and then permanently deleted. Applying retention labels and assigning retention policies helps organizations:

- **Comply proactively with industry regulations and internal policies that require content to be kept for a minimum time.**
- **Reduce risk when there's litigation or a security breach by permanently deleting old content that the organization is no longer required to keep.**
- **Ensure users work only with content that's current and relevant to them. When content has retention settings assigned to it, that content remains in its original location. People can continue to work with their documents or mail as if nothing's changed. But if they edit or delete content that's included in the retention policy, a copy of the content is automatically kept in a secure location. The secure locations and the content are not visible to most people. In most cases, people don't even need to know that their content is subject to retention settings.**

Retention settings work with the following different workloads:

- **SharePoint and OneDrive**
- **Microsoft Teams**
- **Yammer**
- **Exchange**

When using retention policies and retention labels to assign retention settings to content, there are some points to understand about each. Listed below are just a few of the key points. For a more complete list visit Compare capabilities for retention policies and retention labels.

Retention policies

- **Retention policies are used to assign the same retention settings to content at a site level or mailbox level.**
- **A single policy can be applied to multiple locations, or to specific locations or users.**
- **Items inherit the retention settings from their container specified in the retention policy. If a policy is configured to keep content, and an item is then moved outside**

that container, a copy of the item is kept in the workload's secured location. However, the retention settings don't travel with the content in its new location.

Retention labels

- **Retention labels are used to assign retention settings at an item level, such as a folder, document, or email.**
- **An email or document can have only a single retention label assigned to it at a time.**
- **Retention settings from retention labels travel with the content if it's moved to a different location within your Microsoft 365 tenant.**
- **Admins can enable users in the organization to apply a retention label manually.**
- **A retention label can be applied automatically if it matches defined conditions.**
- **A default label can be applied for SharePoint documents.**
- **Retention labels support disposition review to review the content before it's permanently deleted.**

Consider the following scenarios. If all documents in a SharePoint site should be kept for five years, it's more efficient to do with a retention policy than apply the same retention label to all documents in that site.

However, if some documents in that site should be kept for five years and others for 10 years, you'd need to apply a policy to the SharePoint site with a retention period of five years. You'd then apply a retention label to the individual items with a retention setting of 10 years.

Next unit: Describe records management

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Describe records management

3 minutes

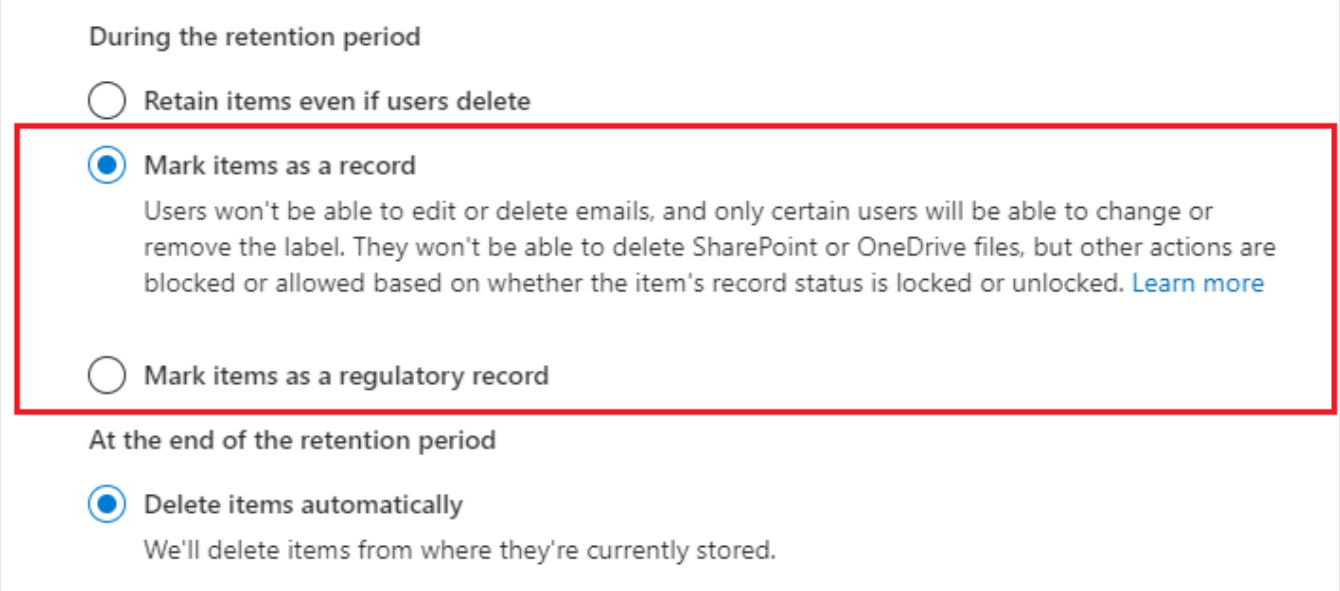
Organizations of all types require a management solution to manage regulatory, legal, and business-critical records across their corporate data. Microsoft Purview Records Management helps an organization look after their legal obligations. It also helps to demonstrate compliance with regulations, and increases efficiency with regular disposition of items that are no longer required to be kept, no longer of value, or no longer required for business purposes. Microsoft Purview Records Management includes many features, including:

- **Labeling content as a record.**
- **Establishing retention and deletion policies within the record label.**
- **Triggering event-based retention.**
- **Reviewing and validating disposition.**
- **Proof of records deletion.**
- **Exporting information about disposed items.**

When content is labeled as a record, the following happens:

- **Restrictions are put in place to block certain activities.**
- **Activities are logged.**
- **Proof of disposition is kept at the end of the retention period.**

To enable items to be marked as records, an administrator sets up retention labels.



Items such as documents and emails can then be marked as records based on those retention labels. Items might be marked as records, but they can also be shown as regulatory records. Regulatory records provide other controls and restrictions such as:

- **A regulatory label can't be removed when an item has been marked as a regulatory record.**
- **The retention periods can't be made shorter after the label has been applied.**

For more information on comparing, use the Compare restrictions for what actions are allowed or blocked section of the documentation.

The most important difference is that if content has been marked as a regulatory record, nobody, not even a global administrator, can remove the label. Marking an item as a regulatory record can have irreversible consequences, and should only be used when necessary. As a result, this option isn't available by default, and has to be enabled by the administrator using PowerShell.

Common use cases for records management

The capabilities of Microsoft Purview Records Management are flexible. There are different ways in which records management can be used across an organization, including:

- **Enabling administrators and users to manually apply retention and deletion actions for documents and emails.**
- **Automatically applying retention and deletion actions to documents and emails.**
- **Enabling site admins to set default retain and delete actions for all content in a SharePoint library, folder, or document set.**
- **Enabling users to automatically apply retain and delete actions to emails by using Outlook rules.**

To ensure records management is used correctly across the organization, administrators can work with content creators to put together training materials. Documentation should explain how to apply labels to drive usage, and ensure a consistent understanding.

Next unit: Knowledge check

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Summary & resources

1 minute

You've explored how Microsoft Purview capabilities like data classification, records management, and data loss prevention can help provide information protection and data lifecycle management across an organization.

Without these capabilities, an organization's information could be at risk, and it might not be compliant with legal and regulatory standards. Microsoft Purview Information Protection and Microsoft Purview Data Lifecycle Management can help organizations address their compliance needs and mitigate risk.

Now that you've completed this module, you should be able to:

- **Describe data classification capabilities.**
- **Describe data loss prevention.**
- **Describe records management.**

Learn more

- Know your data - data classification overview
- Learn about sensitive information types
- Interactive guide - Classify data using sensitive info types with Microsoft Purview Information Protection
- Interactive guide - Identify content using trainable classifiers in Microsoft Purview Information Protection
- Get started with content explorer
- Get started with activity explorer
- Interactive guide - Monitor the use of sensitive information in your organization with Microsoft Purview Information Protection
- Learn about sensitivity labels
- Interactive guide - Create labels and label policies with Microsoft Purview Information Protection
- Learn about data loss prevention
- Learn about retention policies and retention labels
- Govern your data with Microsoft Purview
- Learn about records management

Module complete:

Continue to next module >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Introduction

1 minute

Organizations understand that risks can come from insiders, like contractors, or even employees. There's always a risk that people might share information with competitors after leaving the company. Organizations need to ensure that they're protected from these kinds of risks.

In this module, you'll learn how insider risk management, communication compliance, and information barriers in Microsoft Purview can help you protect your organization.

After completing this module, you'll be able to:

- **Describe insider risk management.**
- **Describe communication compliance.**
- **Describe information barriers.**

Next unit: Describe insider risk management

Continue

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Describe insider risk management

4 minutes

Microsoft Purview Insider Risk Management is a solution that helps minimize internal risks by enabling an organization to detect, investigate, and act on risky and malicious activities. Insider risk management is available in the Microsoft Purview compliance portal.

Managing and minimizing risk in an organization starts with understanding the types of risks found in the modern workplace. Some risks are driven by external events and factors, and are outside an organization's direct control. Other risks are driven by internal events and employee activities that can be eliminated and avoided. Some examples are risks from illegal, inappropriate, unauthorized, or unethical behavior and actions by employees and managers. These behaviors can lead to a broad range of internal risks from employees:

- **Leaks of sensitive data and data spillage**
- **Confidentiality violations**
- **Intellectual property (IP) theft**
- **Fraud**
- **Insider trading**
- **Regulatory compliance violations**

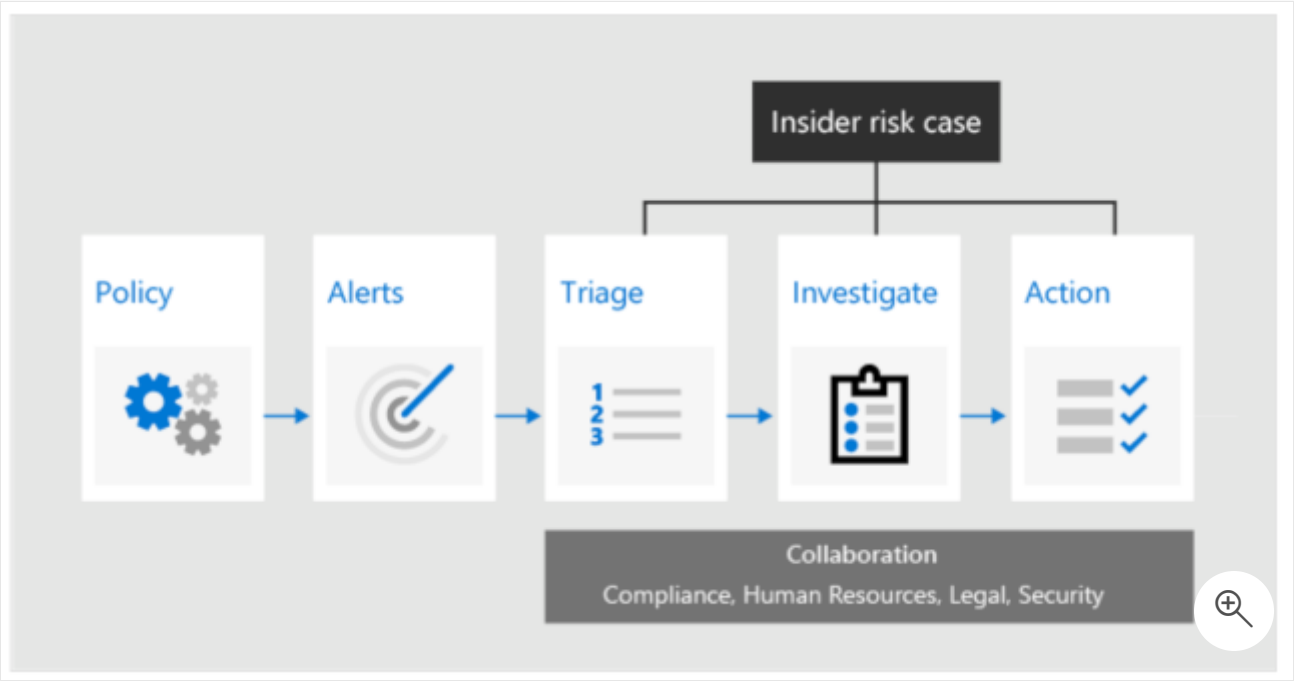
Insider risk management is centered around the following principles:

- **Transparency: Balance user privacy versus organization risk with privacy-by-design architecture.**
- **Configurable: Configurable policies based on industry, geographical, and business groups.**
- **Integrated: Integrated workflow across Microsoft Purview solutions.**
- **Actionable: Provides insights to enable user notifications, data investigations, and user investigations.**

Insider risk management workflow

Insider risk management helps organizations to identify, investigate, and address internal risks. With focused policy templates, comprehensive activity signaling across Microsoft 365, and a flexible workflow, organizations can take advantage of actionable

insights to help identify and resolve risky behavior quickly. Identifying and resolving internal risk activities and compliance issues with insider risk management in Microsoft Purview is achieved using the following workflow:



- **Policies - Insider risk management policies are created using predefined templates and policy conditions that define what risk indicators are examined in Microsoft 365 feature areas. These conditions include how indicators are used for alerts, what users are included in the policy, which services are prioritized, and the monitoring time period.**
- **Alerts - Alerts are automatically generated by risk indicators that match policy conditions and are displayed in the Alerts dashboard. This dashboard enables a quick view of all alerts needing review, open alerts over time, and alert statistics for the organization.**
- **Triage - New activities that need investigation automatically generate alerts that are assigned a *Needs review* status. Reviewers in the organization can quickly identify these alerts and scroll through each to evaluate and triage. Alerts are resolved by opening a new case, assigning the alert to an existing case, or dismissing the alert. As part of the triage process, reviewers can view alert details for the policy match, view user activity associated with the match, see the severity of the alert, and review user profile information.**
- **Investigate - Cases are created for alerts that require deeper review and investigation of the details and circumstances around the policy match. The Case dashboard provides an all-up view of all active cases, open cases over time, and case statistics for the organization. Selecting a case on the dashboard opens it for investigation and review. This area is where risk activities, policy conditions, alerts details, and user details are synthesized into an integrated view for reviewers.**

- **Action - After cases are investigated, reviewers can quickly act to resolve the case or collaborate with other risk stakeholders in the organization.**
  - **Actions can be as simple as sending a notification when employees accidentally or inadvertently violate policy conditions.**
  - **In more serious cases, reviewers may need to share the insider risk management case information with other reviewers in the organization. Escalating a case for investigation makes it possible to transfer data and management of the case to eDiscovery (Premium) in Microsoft Purview.**

Insider risk management can help you detect, investigate, and take action to mitigate internal risks in your organization in several common scenarios. These scenarios include data theft by employees, the intentional, or unintentional leak of confidential information, offensive behavior, and more.

Next unit: Describe communication compliance

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

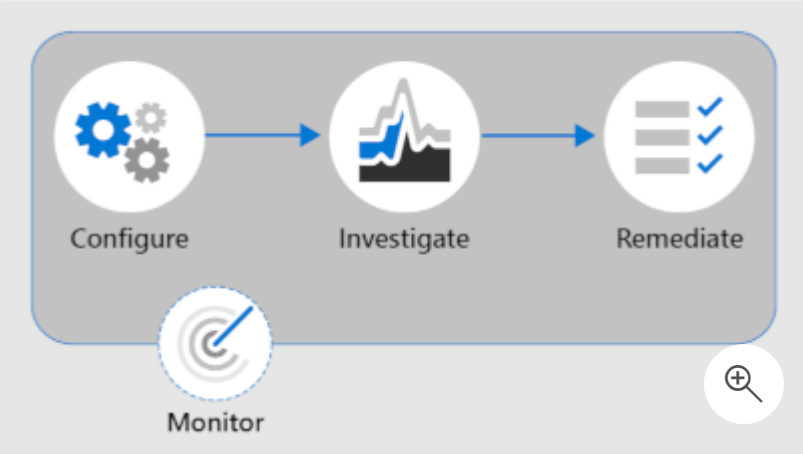
100 XP

Describe communication compliance

10 minutes

Communication compliance in the Microsoft Purview compliance portal helps minimize communication risks by enabling organizations to detect, capture, and take remediation actions for inappropriate messages. Predefined and custom policies in communication compliance make it possible to scan internal and external communications for policy matches so they can be examined by chosen reviewers.

Identifying and resolving compliance issues with communication compliance in Microsoft Purview uses the following workflow:



- **Configure – in this step, admins identify compliance requirements and configure applicable communication compliance policies.**
- **Investigate – admins look deeper into the issues detected when matching your communication compliance policies. Tools and steps that help include alerts, issue management to help remediation, document reviews, reviewing user history, and filters.**
- **Remediate – remediate communications compliance issues. Options include resolving an alert, tagging a message, notifying the user, escalating to another reviewer, marking an alert as a false positive, removing a message in Teams, and escalating for investigation.**
- **Monitor – Keeping track and managing compliance issues identified by communication compliance policies spans the entire workflow process. Communication compliance dashboard widgets, export logs, and events recorded in the unified audit logs can be used to continually evaluate and improve your compliance posture.**

Communication compliance enables reviewers to investigate scanned emails, and messages across Microsoft Teams, Exchange Online, Yammer, or third-party communications in an organization, taking appropriate remediation actions to make sure they're compliant with the organization's message standards.

Some important compliance areas where communication compliance policies can assist with reviewing messages include:

- **Corporate policies - Users have to follow corporate policies like usage and ethical standards in their day-to-day business communications. With communication compliance, admins can scan user communications across the organization for potential concerns of offensive language or harassment.**
- **Risk management - Communication compliance can help admins scan for unauthorized communication about projects that are considered to be confidential, such as acquisitions, earnings disclosures, and more.**
- **Regulatory compliance - Most organizations are expected to follow some regulatory compliance standards during their day-to-day operations. For example, a regulation might require organizations to review communications of its brokers to safeguard against potential insider trading, money laundering, or bribery. Communication compliance enables the organization to scan and report on these types of communications in a way that meets their requirements.**

Watch the video below for a walk-through of Microsoft Purview Communication Compliance.

> **Note**
>
> **The user interface (UI) in Microsoft 365 is continually evolving so the UI shown in the video may not reflect the most recent updates.**

Communication compliance is a powerful tool, that can help maintain and safeguard your staff, your data and your organization.

Next unit: Describe information barriers

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Describe information barriers

3 minutes

Microsoft 365 provides organizations with powerful communication and collaboration capabilities. However, an organization might want to restrict communications between some groups to avoid a conflict of interest from occurring in the organization, or to restrict communications between certain people to safeguard internal information. With information barriers, the organization can restrict communications among specific groups of users.

Microsoft Purview Information Barriers is supported in Microsoft Teams, SharePoint Online, and OneDrive for Business.

Information barriers are policies that admins can configure to prevent individuals or groups from communicating with each other. When information barrier policies are in place, people who shouldn't communicate with other specific users can't find, select, chat, or call those users. With information barriers, checks are in place to prevent unauthorized communication.

> **Note**
>
> **It's important to note that information barriers *only support two-way restrictions*. One-way restrictions, such as marketing, can communicate with day traders but day traders who can't communicate with marketing are *not supported*.**

Here are some examples of how information barriers can be applied:

- **Education: Students in one school can't look up contact details for students of other schools.**
- **Legal: Maintaining confidentiality of data obtained by the lawyer of one client from being accessed by a lawyer for the same firm representing a different client.**
- **Professional services: A group of people in a company is only able to chat with a client or specific customer via federation or guest access during a customer engagement.**

Information barriers in Microsoft Teams

In Microsoft Teams, information barrier policies determine and prevent the following kinds of unauthorized communications:

- **Searching for a user**
- **Adding a member to a team**
- **Starting a chat session with someone**
- **Starting a group chat**
- **Inviting someone to join a meeting**
- **Sharing a screen**
- **Placing a call**
- **Sharing a file with another user**
- **Access to file through sharing link**

If the people involved are included in an information barrier policy to prevent the activity, they can't continue. Potentially, everyone included in an information barrier policy can be blocked from communicating with others in Microsoft Teams. When people affected by information barrier policies are part of the same team or group chat, they might be removed from those chat sessions and further communication with the group might not be allowed.

To learn more about the user experience with information barriers, see information barriers in Microsoft Teams.

Next unit: Knowledge check

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Summary and resources

1 minute

There are various capabilities available from Microsoft Purview to help protect organizations from data leaks or inappropriate communication, from company insiders.

Now that you've completed this module, you should be able to:

- **Describe insider risk management.**
- **Describe communication compliance.**
- **Describe information barriers.**

Learn more

- **Learn about insider risk management**
- **Get started with communication compliance**
- **Information barriers**

Module complete:

Unlock achievement

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Introduction

1 minute

Organizations may need to identify, collect, and/or audit information for legal, regulatory, or business reasons. With today's volume and variety of data, it's vital that an organization can do this in an efficient and timely manner. The eDiscovery and audit capabilities in Microsoft Purview can help organizations to achieve this goal.

Learn how the eDiscovery and audit capabilities of Microsoft Purview help organizations find relevant data quickly.

In this module, you'll learn about the eDiscovery capabilities in Microsoft 365.

After completing this module, you'll be able to:

- **Describe the eDiscovery solutions in Microsoft Purview.**
- **Describe the auditing solutions in Microsoft Purview.**

Next unit: Describe the eDiscovery solutions in Microsoft Purview

Continue

100 XP

Describe the eDiscovery solutions in Microsoft Purview

3 minutes

Electronic discovery, or eDiscovery, is the process of identifying and delivering electronic information that can be used as evidence in legal cases. You can use eDiscovery tools in Microsoft Purview to search for content in Exchange Online, OneDrive for Business, SharePoint Online, Microsoft Teams, Microsoft 365 Groups, and Yammer teams. You can search mailboxes and sites in the same eDiscovery search, and then export the search results. You can use eDiscovery cases to identify, hold, and export content found in mailboxes and sites.

Microsoft Purview provides three eDiscovery solutions: Content search, eDiscovery (Standard), and eDiscovery (Premium).

- **Content Search. Use the Content search tool to search for content across Microsoft 365 data sources and then export the search results to a local computer.**
- **eDiscovery (Standard). The eDiscovery (Standard) solution builds on the basic search and export functionality of Content search by enabling you to create eDiscovery cases and assign eDiscovery managers to specific cases. The eDiscovery (Standard) solution also lets you associate searches and exports with a case and lets you place an eDiscovery hold on content locations relevant to the case.**
- **eDiscovery (Premium). The eDiscovery (Premium) solution builds on the existing capabilities in eDiscovery (Standard). In addition, eDiscovery (Premium) provides an end-to-end workflow to identify, preserve, collect, review, analyze, and export content that's responsive to your organization's internal and external investigations. It lets legal teams manage custodians, people that you've identified as people of interest in the case, and the workflow to communicate with custodians. It allows you to collect and copy data into review sets, where you can filter, search,**

and tag content so you can identify and focus on content that's most relevant. The eDiscovery (Premium) solution provides analytics and machine learning-based predictive coding models to further narrow the scope of your investigation to the most relevant content.

Subscriptions that support eDiscovery (Standard) also support Content search. Subscriptions that support eDiscovery (Premium) also support Content search and eDiscovery (Standard).

To access any of the eDiscovery-related tools, a user must be assigned the appropriate permissions. Specifically, a user must be added as a member of the eDiscovery Manager role group in the Microsoft Purview compliance portal.

Next unit: Describe the audit solutions in Microsoft Purview

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

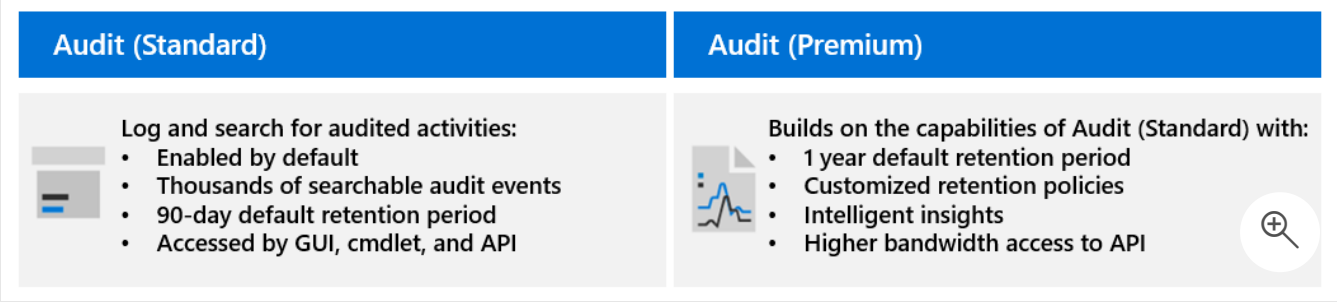
100 XP

Describe the audit solutions in Microsoft Purview

3 minutes

Auditing solutions in Microsoft Purview help organizations effectively respond to security events, forensic investigations, internal investigations, and compliance obligations. Thousands of user and admin operations performed in dozens of Microsoft 365 services and solutions are captured, recorded, and retained in your organization's unified audit log. Audit records for these events are searchable by security ops, IT admins, insider risk teams, and compliance and legal investigators in your organization. This capability provides visibility into the activities performed across your Microsoft 365 organization.

Microsoft Purview provides two auditing solutions: Audit (Standard) and Audit (Premium).



- **Audit (Standard). Audit (Standard) provides you with the ability to log and search for audited activities and power your forensic, IT, compliance, and legal investigations. Audit (Standard) is turned on by default for all organizations with the appropriate subscription. You can search for a wide-range of audited activities that occur in most of the Microsoft 365 services in your organization. Audit records can also be retrieved using the Office 365 Management Activity API. You can export the audit records returned by the search, to a CSV file, enabling further analysis using Microsoft Excel or Excel Power Query. In Audit (Standard), records are retained for 90 days.**

- **Audit (Premium). Audit (Premium) builds on the capabilities of Audit (Standard). Audit (Premium) provides audit log retention policies and longer retention of audit records. It provides intelligent insights that can help you investigate possible breaches and determine the scope of compromise. Audit (Premium) also provides**

organizations with more bandwidth to access auditing logs through the Office 365 Management Activity API.

It can take anywhere from 30 minutes to 24 hours after an event occurs for the corresponding audit log record to be returned in the results of an audit log search.

Licensing for Audit (Standard) or Audit (Premium) requires the appropriate organization-level subscription and corresponding per-user licensing. For additional information on licensing requirements, visit the Learn more section in the Summary and resources unit.

Admins and members of investigation teams must be assigned the View-Only Audit Logs or Audit Logs role in Exchange Online to search the audit log. By default, these roles are assigned to the Compliance Management and Organization Management role groups on the Permissions page in the Exchange admin center.

Next unit: Knowledge check

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Summary and resources

1 minute

The eDiscovery and audit solutions in Microsoft Purview can help organizations identify, collect, and audit information in a rapid and effective manner, to meet legal requirements.

Now that you've completed this module, you'll be able to:

- **Describe the eDiscovery solutions in Microsoft Purview.**
- **Describe the auditing solutions in Microsoft Purview.**

Learn more

- **Microsoft Purview eDiscovery solutions**
- **Search for content using the Content search tool**
- **Get started with eDiscovery (Standard) in Microsoft Purview**
- **Overview of Microsoft Purview eDiscovery (Premium)**
- **Auditing solutions in Microsoft Purview**
- **Microsoft Purview Audit (Premium)**
- **Turn audit log search on or off**

100 XP

Introduction

1 minute

Azure has the capabilities that admins need to ensure that resources are governed properly, that they're secure, and in line with the organization's compliance requirements.

In this module, you'll learn about the resource governance capabilities available for Azure.

After completing this module, you'll be able to:

- **Describe Azure Policy.**
- **Describe Azure Blueprints.**
- **Describe the capabilities in the Microsoft Purview governance portal.**

Next unit: Describe Azure Policy

Continue

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Describe Azure Policy

3 minutes

Azure Policy is designed to help enforce standards and assess compliance across your organization. Through its compliance dashboard, you can access an aggregated view to help evaluate the overall state of the environment. You can drill down to a per-resource, or per-policy level granularity. You can also use capabilities like bulk remediation for existing resources and automatic remediation for new resources, to resolve issues rapidly and effectively. Common use cases for Azure Policy include implementing governance for resource consistency, regulatory compliance, security, cost, and management.

Azure Policy evaluates all resources in Azure and Arc enabled resources (specific resource types hosted outside of Azure).

Azure Policy evaluates whether the properties of resources match with business rules. These business rules are described using JSON format, and referred to as policy definitions. For simplified management, you can group together multiple business rules to form a single policy initiative. After business rules have been formed, you can assign the policy definition, or policy initiative, to any scope of resources that are supported, such as management groups, subscriptions, resource groups, or individual resources.

Evaluation outcomes

Azure Policy evaluates resources at specific times during the resource lifecycle and the policy assignment lifecycle, and for regular ongoing compliance evaluation. The following events or times will trigger an evaluation:

- **A resource has been created, deleted, or updated in scope with a policy assignment.**
- **A policy or an initiative is newly assigned to a scope.**
- **A policy or an initiative that's been assigned to a scope is updated.**
- **The standard compliance evaluation cycle (happens once every 24 hours).**

Organizations will vary in how they respond to non-compliant resources. Here's some examples:

- **Deny a change to a resource.**
- **Log changes to a resource.**
- **Alter a resource before or after a change.**
- **Deploy related compliant resources.**

With Azure Policy, responses like these are made possible by using effects, which are specified in policy definitions.

What's the difference between Azure Policy and Azure role-based access control (RBAC)?

It's important not to confuse Azure Policy and Azure RBAC. You use Azure Policy to ensure that the resource state is compliant to your organization's business rules, no matter who made the change or who has permission to make changes. Azure Policy will evaluate the state of a resource, and act to ensure the resource stays compliant.

Azure RBAC focuses instead on managing user actions at different scopes. Azure RBAC manages who has access to Azure resources, what they can do with those resources, and what areas they can access. If actions need to be controlled, then you would use Azure RBAC. If an individual has access to complete an action, but the result is a non-compliant resource, Azure Policy still blocks the action.

Azure RBAC and Azure Policy should be used together to achieve full scope control in Azure.

Next unit: Describe the use of Azure Blueprints

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Describe the use of Azure Blueprints

1 minute

Azure Blueprints provide a way to define a repeatable set of Azure resources. Azure Blueprints enable development teams to rapidly provision and run new environments, with the knowledge that they're in line with the organization's compliance requirements. Teams can also provision Azure resources across several subscriptions simultaneously, meaning they can achieve shorter development times and quicker delivery.

Azure Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts such as:

- **Role Assignments**
- **Policy Assignments**
- **Azure Resource Manager templates (ARM templates)**
- **Resource Groups**

Blueprint objects are replicated to multiple Azure regions. This replication provides low latency, high availability, and consistent access to your blueprint objects, whatever region Azure Blueprints deploys your resources to.

With Azure Blueprints, the relationship between the blueprint definition (*what should be deployed*) and the blueprint assignment (*what was deployed*) is preserved. This connection supports improved tracking and auditing of deployments.

Azure Blueprints helps ensure Azure resources are deployed in a way that's in line with compliance requirements. However, a service like Azure Policy should be used to continuously monitor resources and ensure a continuation with compliance requirements.

Next unit: Describe the capabilities in the Microsoft Purview governance portal

Continue

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Describe the capabilities in the Microsoft Purview governance portal

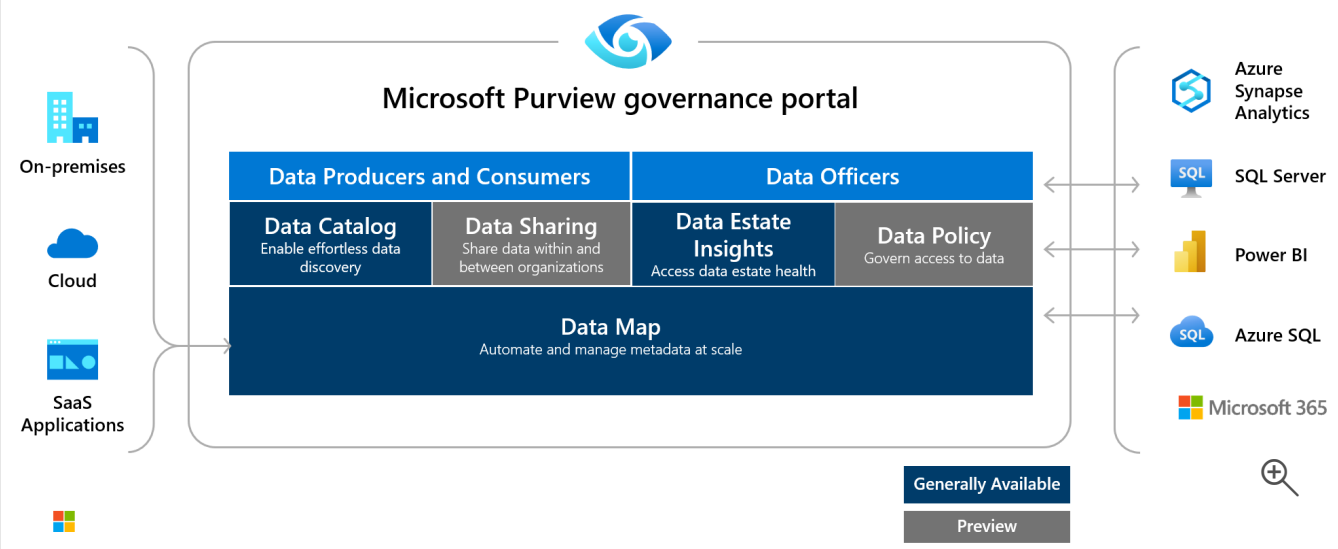
3 minutes

An organization's data is constantly growing and users are storing and sharing data in new directions. For security and compliance administrators, the task of discovering, protecting, and governing sensitive data is one that never ends. The growth of data, also represents challenges for data consumers who might be unaware of a data source. For data producers, those who are responsible for producing and maintaining information assets, creating and maintaining documentation for data sources is complex and time-consuming. Restricting access to data sources and ensuring that data consumers know how to request access is an ongoing challenge.

Microsoft Purview is designed to address the challenges associated with the rapid growth of data and to help enterprises get the most value from their information assets.

The Microsoft Purview governance portal provides a unified data governance service that helps you manage your on-premises, multicloud, and software-as-a-service (SaaS) data. The Microsoft Purview governance portal allows you to:

- **Create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage.**
- **Enable data curators to manage and secure your data estate.**
- **Empower data consumers to find valuable, trustworthy data.**



Data Map

Microsoft Purview Data Map provides the foundation for data discovery and data governance. By scanning registered data sources, Azure Purview Data Map is able to capture metadata about enterprise data, to identify and classify sensitive data. Microsoft Purview supports Azure data sources and various data source categories including databases, file storage, and applications and services from third parties.

Data Catalog

With the Microsoft Purview Data Catalog, business and technical users can quickly and easily find relevant data using a search experience with filters based on various lenses like glossary terms, classifications, sensitivity labels and more.

Data Estate Insights

With the Microsoft Purview Data Estate Insights, data officers and security officers can get a bird's eye view and at a glance understand what data is actively scanned, where sensitive data is, and how it moves.

Data Sharing and Data Policy (preview)

Microsoft Purview Data Sharing enables organizations to securely share data both within your organization or cross organizations with business partners and customers.

Access policies in Microsoft Purview enable you to manage access to different data systems across your entire data estate. For example, if a user needs read access to an Azure Storage account that has been registered in Microsoft Purview, you can grant this access directly in Microsoft Purview by creating a data access policy through the Policy management app in the Microsoft Purview governance portal.

Next unit: Knowledge check

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Summary & resources

1 minute

You've seen how admins can use the resource governance capabilities in Azure to ensure that resources for their organization are governed properly, so that they're secure, and in line with the organization's compliance requirements.

Now that you've completed this module, you'll be able to:

- **Describe Azure Policy.**
- **Describe Azure Blueprints.**
- **Describe the capabilities in the Microsoft Purview governance portal.**

Learn more

- **What is Azure Policy?**
- **What is Azure Blueprints?**
- **What is available in the Microsoft Purview governance portal?**
- **Azure Storage in-place data sharing with Microsoft Purview (preview) Concepts for Microsoft Purview data owner policies**

Module complete:

Unlock achievement

How are we doing? ☆ ☆ ☆ ☆ ☆